JOURNAL OF BUSINESS AND ACCOUNTING

Volume 14, Number 1 ISSN 2153-6252 Fall 2021

IN THIS ISSUE

A REFEREED PUBLICATION OF THE AMERICAN SOCIETY OF BUSINESS AND BEHAVIORAL SCIENCES

JOURNAL OF BUSINESS AND ACCOUNTING
P.O. Box 502147, San Diego, CA 92150-2147: Tel 909-648-2120
Email: mondal@asbbs.org www.asbbs.org
ISSN 2153-6252

The Journal of Business and Accounting is a publication of the American Society of Business and Behavioral Sciences (ASBBS). Papers published in the Journal went through a blind-refereed review process prior to acceptance for publication. The editors wish to thank anonymous referees for their contributions.

The national annual meeting of ASBBS is held in Las Vegas in February/March of each year and the international meeting is held in June/July of each year. Visit www.asbbs.org for information regarding ASBBS.

JOURNAL OF BUSINESS AND ACCOUNTING

ISSN 2153-6252
Volume 14, Number 1 Fall 2021

TABLE OF CONTENTS

Journal of Business and Accounting
Vol 14, No 1; Fall 2021

PREVENTING EMPLOYEE FRAUDS IN SMALL BUSINESSES WITH LOW-COST METHODS

Gregory W. Treadwell
Cameron University

ABSTRACT

Large businesses employ layers of managers, have an abundance of internal controls, and provide employee oversight. In contrast, many small business managers are unwilling or unable to spend existing funds to develop internal controls or provide employee oversight. For these and other reasons, desperate or disgruntled employees often target small businesses. Therefore, the purpose of this study was to reduce small business fraud by identifying what assets motivated employees choose to misappropriate. Then, to determine how motivated employees steal employer assets and to identify what these perpetrators purchase with the stolen items once converted to cash. This emerging information can then help managers of small businesses identify and implement low-cost methods that can help prevent small business employee fraud. Low-cost fraud reduction methods that small companies often adopt include purchasing employee theft insurance, adopting a code of conduct, implementing acceptable hiring practices, and hiring office workers with fraud training. Management may also choose to establish a fraud reporting system and train managers to question why documents are missing or manipulated. Finally, management should learn to listen and look for fraud and use exit interviews to identify ongoing fraudulent activities.

Keywords: Employee fraud, small business frauds, preventing small business frauds, low-cost fraud controls

INTRODUCTION

Without a doubt, most small business employees are trustworthy. Many work to support family members, maintain lifestyles, and build personal wealth. Unfortunately, some good employees will make bad decisions or encounter overwhelming emotional problems. When these situations emerge, the affected employee may discover they are in desperate need of money. Some of these employees will ask family or friends for help. Those that receive support may be able to solve their problem. However, family and friends may also decline other employees'

requests for assistance. In addition, some employees may refuse to ask or be too embarrassed to ask for help. Thus, committing fraud may be the only choice for some employees. Consequently, employees are responsible for approximately 80% of organizational fraud losses (Boyle, Boyle, & Mahoney, 2015).

While large organizations generally have the resources and knowledge to prevent, detect, or deter employee fraud, small businesses lack the resources to avert these motivated employees. In reality, small businesses often have limited resources, a lack of awareness, and a tendency to place too much trust in employees (ACFE, 2020). As a result, 77% of fraud perpetrators work in operations, accounting, executive management, sales, customer service, administrative support, finance, or purchasing (ACFE, 2020). In addition, frauds commonly occur in financial services, municipalities or governments, manufacturing, real estate or construction, labor unions, healthcare, retail, or telecom businesses (Hiscox, 2017).

When an employee commits fraud, public knowledge of the scam can also damage the defrauded businesses. This knowledge may impair the brand, create a loss of market position, lower employee morale, or limit future opportunities (PwC, 2020). It may also force management to reduce salaries and benefits, terminate employees, or eliminate future job opportunities. If sales also decline, management may have to increase sales prices and risk losing customers to competitors. Thus, frauds may compel management to liquidate assets, or worse, file for bankruptcy (Peltier-Rivest & Lanoue, 2012).

If management chooses not to prosecute a suspected perpetrator, the decision is often based on the belief that internal discipline is sufficient or that litigation would be too costly (Brody, 2010). However, when a defrauded business chooses to dismiss an alleged perpetrator without prosecution, that individual can quickly move on to steal from other unsuspecting companies. Knowledge of the dismissal may also cause the remaining employees to view management's non-prosecution attitude as an invitation to commit additional fraudulent acts.

Therefore, when a small business has limited controls, an abundance of trust, or inadequate oversight, management must understand that any employee with sufficient needs may become motivated to commit fraud. Thus, employee frauds in small businesses are a problem. As a result, this study addressed the limited ability of small businesses to prevent, detect, or deter employee fraud. The study also suggests that small companies adopt strategies for preventing fraud before it starts. In addition, the purpose of this study was to identify what assets motivated

employees misappropriated, what methods these employees implemented to steal employer assets, and what these perpetrators purchased with the stolen items after converting them to cash. The study implemented a qualitative approach to gather information from multiple fraud cases to identify perpetrators' behaviors to obtain this information. Then use the emerging information to develop a list of low-cost methods that small businesses could implement to prevent, detect, or deter employees from committing fraud. T

LITERATURE REVIEW

Small business managers commonly focus on providing services, manufacturing or selling products, conducting research and development, and ensuring customers are pleased with the products or services. These small business managers may believe employee fraud is a problem for other businesses–not theirs (Henry, 2016). However, all organizations are at risk of becoming a target for employees (Murdock, 2008). So, when a small business fraud occurs, it is often the result of inadequate resources to implement proactive fraud prevention and detection methods (Ruggieri, 2012). This lack of resources may reduce the ability of small business managers to provide a thorough oversight (Hrncir & Metts, 2012) or inadequate training that could prevent or detect employee fraud (Sims, 2010).

Employees may become motivated to commit fraud when there are inadequate controls, poor training, poor supervision, ineffective anti-fraud programs, or weak ethical cultures at the worksite (Dorminey, Fleming, Kranacher, and Riley, 2010). Motivations can include employees who believe they need a reward. An example would consist of an employee who expected but failed to receive a pay raise or bonus; so, they decided to get the raise or bonus fraudulently. Employees may also be motivated to commit fraud if they feel unappreciated or overworked. There are also employees that believe they are more intelligent than the boss and attempt to prove their superior intellect by stealing business assets (Ulmer & Noe, 2013). Employees will also commit fraud to project the appearance of being wealthy or when they cannot delay a need for self-gratification. Then there are employees that commit fraud to remedy judgments, weather-related damages, or unforeseen medical bills. Employees are also motivated to commit fraud to fund immoral acts. These motivations often include excessive gambling, legal or illegal drug habits, or extramarital affairs.

However, before most employees commit fraud, they need an opportunity that will enable them to avoid job losses and the possibility of prosecution (Dorminey et al., 2010). Employees' access to assets often provides them with the required opportunity. The opportunity to commit fraud may also occur when an employee intentionally overrides internal controls or managers provide insufficient

oversight. Insufficient oversight is often the byproduct of inadequate training, poor supervision, a history of not prosecuting perpetrators, ineffective anti-fraud programs, or a weak ethical culture (Dorminey et al., 2010). In addition, small business managers that rely on too much trust may quickly learn that employees with personal needs, access to business assets, and the ability to justify the theft–do misappropriate assets. As a result, the ACFE estimates that organizations lose 5% of revenues to fraud (ACFE, 2020).

The perpetrators of employee frauds commonly do not see themselves as criminals but as victims of circumstances. So, they must rationalize fraudulent behaviors before committing the fraud (Dorminey et al., 2010). Rationalization is a mental process that enables employees to replace customary beliefs with actions that appear more rational. For example, employees will misappropriate cash and justify the act as a borrowing activity that they plan to repay sometime in the future. Unfortunately, that time never arrives! In effect, rationalization is probably the most dangerous element of fraud since it is nearly impossible for management to eliminate how employees think (Coenen, 2008).

Furthermore, the ability to conceal misappropriations can also decrease the likelihood of management detecting fraudulent acts. Concealment methods can include an employee consuming inventory items while at work or hiding items in purses or lunch boxes as employees leave for the day. More energetic employees may choose to conceal stolen items in interior trash containers and retrieve the valuables from the dumpster and under cover of darkness. Alternatively, employees with access to inventory may take what they want and blame the shortage, if discovered, on over shipments to customers. Then, employees with access to inventory and accounting records may misappropriate inventory and then manipulate the amounts by creating false journal entries, fictitious source documents, manipulated documents, or actually destroy documents.

The managers of small businesses also need to understand that employees can be predatory or accidental fraudsters. Predatory individuals accept job offers with the sole intent to misappropriate assets. Predators have previously committed fraudulent acts and only need an opportunity to commit another fraud (Kapp & Heslop, 2011), which often depends upon convincing another unsuspecting manager to hire them. In contrast, accidental fraudsters start jobs with honorable intentions; however, they encounter a non-shareable financial problem after being hired. To solve the emerging problem, that employee may develop a perceived opportunity and a morally defensible excuse for stealing employer assets (Dorminey, Fleming, Kranacher, and Riley, 2012a). These perpetrators are often first-time offenders, middle-aged, well-educated, trusted, and in a position of responsibility (Dorminey et al., 2010).

Finally, employees often demonstrate *warning signs* before misappropriating assets (Hrncir & Metts, 2012).
Common warning signs of fraud can include living beyond their means, a substantial lifestyle change, becoming too possessive of work records, reluctant to share tasks, apprehensive about using vacations or time off, always being the first in the office and the last to leave, showing signs of substance abuse, or holding grudges against employers—whether justified or not (Klein, 2015).
Thus, small business managers need to be on the lookout for behavioral changes in employees. In support, the ACFE reported that warning signs were present in 85% of fraud cases, and multiple warning signs were present in 49% of the fraud cases (2020). (See Table #1)

Table #1: Behavioral Red Flags Displayed by Perpetrators

Behaviors	Percentages
Living beyond means	42%
Financial Difficulties	26%
Unusually close association with vendor/customer	19%
No behavior red flags	15%
Control issues, unwillingness to share duties	15%
Irritability, suspiciousness, or defensiveness	13%
"Wheeler-dealer" attitude	13%
Divorce/family problems	12%
Addiction problems	9%
Complained about inadequate pay	8%
Refusal to take vacations	7%
Excessive pressure from within the organization	7%
Past employment-related problems	6%
Social isolation	6%
Complained about last of authority	5%
Past legal problems	5%
Excessive family/peer pressure for success	4%
Instability in life circumstances	4%
Others	4%

Source: 2020 ACFE Report to the Nations

METHODOLOGY

This study implemented a qualitative research design to explore data from multiple employee fraud cases perpetrated in the United States. The search group included small business employee fraud cases identified by the Google browser. Search phrases included employee fraud cases, employee fraud sentencing, and employee fraud case sentencing. Excluded cases included those that did not appear to be a small business fraud. Then from each identified small business fraud case,

multiple articles or reports were obtained and triangulated to confirm the information's accuracy and to identify common characteristics. The chosen articles and reports included radio station reports, newspaper reports, FBI reports, IRS reports, Department of Justice Reports, and various State Court Reports.

The identification of acceptable cases continued until the new cases were no longer providing additional data. The additional data categories included (1) additions to the kinds of misappropriated assets, (2) changes in methods used to misappropriate assets, (3) changes to areas the perpetrators worked in, (4) and what the perpetrator bought with the misappropriate item or funds.

RESULTS

Of the 40 chosen cases, all of the defendants pled guilty or were adjudicated guilty of fraud. Among the 40 cases, 34 accepted cases involved small business frauds perpetrated by office workers. (See Table #2) Of the two remaining acceptable cases, one involved the perpetrator buying equipment and parts with business funds. Those items were subsequently misappropriated and taken to the employee's home for personal use. The final accepted case involved an employee purchasing unnecessary inventory for the business; however, the employee sold those items on the internet and pocketed the proceeds.

Three of the four remaining cases involved managers or owners falsifying or submitting false documents to increase business revenues. These cases were management frauds, so they were omitted. The last excluded case involved a vendor that attempted to swindle small business employees by compelling them to purchase fictitious investments.

Table #2: Job Titles of Office Worker that Perpetrated Frauds
Billing Clerk
Accounts Receivable Clerk
Payroll Clerk
Payroll Specialist
Support Worker or Specialist
Controller
Office Manager
Bookkeeper
Director
Date Entry Clerk
Sales Person or Sales Manager
Manager
Document Manager or Document Technician
Assistant
Accountant
Accounts Payable Clerk
Supervisor

This case was a vendor fraud so, it was also excluded from the study. Of the acceptable 36 cases, the perpetrators misappropriate assets using various methods. Those methods included: (See Table #3)

Table #3: Methods Used by Perpetrators to Misappropriate Employer Assets
Issued checks payable to themselves.
Issued payroll checks to "Ghost Employee."
Made unauthorized purchases with the Business Credit Cards or Debit cards
Stole checks payable to the employer and deposited them into a new account opened fraudulently at another bank.
Made unauthorized wire transfers
Clerk pilfered the Petty Cash.
Purchased unnecessary equipment and sold it online.
After collecting the sales amount, the clerk re-rings the sale with a discount.
Departing employees Credit Card were kept by office personal who used the credit cards to make personal purchases.
Complete and submit new credit card applications without the owner's knowledge
Instruct Payroll Business to issue additional salary/bonus payments
Stole current or former employees' personal information and sold or used it to obtain money.
Purchased and then sold parts and equipment for home use.
Purchased unnecessary inventory and then sold the items on the internet.

Of the chosen cases, the perpetrator chose a variety of items to purchase. Those purchases included: (See Table #4)

Table #4: Perpetrators' Purchases with Misappropriated Funds
Gambling
New Vehicles (Cars, Trucks, Tractors, RV, Motorcycles)
New Home/Remodel Home
Vacations/Travel
Credit Card and Mortgage Payments
Drugs
Personal Living Expenses
To Build or Grow Personal Business
Sporting Events/Concerts
Lavish lifestyle
Gift Cards
Jewelry

DISCUSSION

Many of the reviewed cases indicated that judges and attorneys associated with the cases believed an overreliance on trust or a lack of management oversight partly enabled the fraud to occur. Regrettably, they

did not comment on whether insufficient funds or an unwillingness of managers to spend funds contributed to the fraudulent activity. However, it was evident that the small business managers needed internal controls beyond those currently used to prevent future frauds. Thus, the recommendations emerging from this study suggest that small businesses with limited funds should attempt to implement low-cost controls that can prevent, detect, or deter employee fraud.

Small businesses should adopt some basic rules regarding incoming mail and deposits. The mail should be delivered to or retrieved by management, not an employee who has access to accounting records. Management should personally destroy all unwanted credit card applications and unsolicited loan offers. Cash receipts should be deposited in the bank by someone who does not have access to accounting records. Management should compare the validated deposit receipts amounts with the dollar amount of funds sent to the bank to make sure they are in agreement. Management should also verify that the deposit went into the correct account and the correct bank. Signature stamps or plates should be locked in a vault so unauthorized employees cannot write and sign unauthorized checks. In addition, management should separate duties in areas where they keep cash, store records, transactions occur, and employees prepare reconciliations.

The management of small businesses should also consider purchasing employee dishonesty or employee theft insurance. If purchased, the insurance policy could protect the businesses from theft by one or more employees. The policy may also enable the business to recover losses of money, securities, or property. In addition, these policies may protect the businesses from losses associated with forgeries, fraud, embezzlement, or unauthorized electronic transfers.

Small business managers should also create and adopt a code of conduct. The adopted code should discuss management's attitude toward fraud and what actions will occur if an employee commits a fraudulent act. Once adopted, management should display the code of conduct in common areas so any employee can read the document. In addition, a publicly displayed code of conduct can become a fraud deterrent method since it sends the message that management is looking for fraud and employees that know management is looking for fraud will not risk losing their job.

Hiring honest employees is one of the most prudent ways for employers to protect business assets, revenues, and sensitive data (Brody, 2010). Consequently, managers of small businesses should adopt procedures that limit poor hiring practices. Reasonable hiring procedures often include using reputable internet job sites or local employment agencies to identify quality employees.

After identifying an acceptable candidate, the small business managers should verify that candidate's employment, education, certifications, credit, and references. In contrast, small business managers should not blindly accept a current employee's recommendation to hire a relative or acquaintance. While an employee's recommendation may produce a highly qualified employee, it may also produce a new employee that owes the recommending employee a favor. That favor may include collusion to override controls, making it easier for the recommending employee to misappropriate assets.

Additionally, when small business managers look for accounting or management employees, they should consider hiring qualified candidates that have also completed a collegiate fraud examination course. If successful, the new employee could teach management about the risks of fraud and fraud deterrence methods (Peterson, 2003). They may also know how employees misappropriate assets in particular businesses and understand how they conceal those thefts. Employees armed with fraud knowledge could help prevent future frauds by identifying where additional low-cost fraud controls would be helpful. Hence, education is an essential element that can help prevent criminal activities (Groot & van den Brink, 2010).

Small business managers should also develop a fraud reporting mechanism to enable employees to report suspicious activities. The resulting employee tips could help uncover over 40% of the frauds (ACFE, 2020). The emerging system could begin with one or more well-made boxes with a hinged top and a locking mechanism. The top of each box would have a small opening enabling employees to submit written notes describing suspicious activities anonymously. The reporting boxes would need to be firmly attached to a wall or sturdy piece of furniture to prevent theft and placed in an area where fellow employees would not observe the insertion of notes. Once in place, a specific manager would lock the boxes and retain the only key. Periodically, that same manager would return to the reporting boxes, retrieve any deposited notes, review the notes, and decide if any action is necessary. However, before installing the reporting boxes, all employees would need to receive a briefing on the purpose and proper use of the boxes. Once in place, all employees should recognize that management is on the lookout for suspicious activities; thus, fewer fraudulent acts should occur. Management may also enhance the reporting mechanism by enabling employees to receive monetary rewards for accurately reporting suspicious activities that lead to prosecution. However, the collection of rewards may require the reporting employee to give up their anonymity.

Small business managers should also recognize that most employees will not commit fraud if they cannot conceal the fraudulent activities. Concealment represents deliberate actions to hide the fraud (Dorminey et al., 2012a), and these methods often include manipulating, hiding, or destroying documents; or suppressing material facts to defraud an employer. For example, manipulated

documents can include falsified document information, forged signatures, or fictitious numbers. Without the ability to conceal the fraudulent activities may diminish. For example, management may easily detect the fraudulent acts, which could cause embarrassment among family members, job losses, and legal issues for the perpetrator. Therefore, small business managers should always review and question why documents are missing or manipulated.

Management should also reduce the ability of employees to conceal fraudulent acts by requiring all employees to take annual vacations. This policy would enable a substitute worker to have one or two weeks to perform the vacationing employees' duties and identify any irregularities. Management could also adopt a job rotation policy for specific jobs that would rotate employees from job to job; thus, reducing an employee's ability to favor particular vendors or customers and possibly reducing or eliminate kickback schemes.

Management should also watch for signals that suggest fraudulent activities may be occurring. In support, a former police officer and certified fraud examiner stated that inside fraud information comes from watching, listening, and evaluating others under ordinary circumstances (Nance, 2003). The act of looking and listening for fraud opportunities, motivations, concealment methods, or watching for red flags can include management by wandering around (MBWA). MBWA is a method used by managers to get out of the office, exercise, and use that opportunity to talk with workers (Katopol, 2018). For fraud detection purposes, the MBWA practice could enable managers to watch for fraudulent acts, listen for employees talking about desperation situations, or make themselves available for any worker to discuss suspicious activities with the boss.

While most cases in this study involved cash, two cases involved non-cash thefts. To prevent these non-cash thefts, management should make it difficult for employees to remove misappropriated items from the worksite. While locked doors and limited entry and exits may reduce thefts, they also increase the chances of bodily harm for employees in the event of a fire or severe weather. Therefore, a better idea could include moving employee parking away from exit doors. In addition, management could require all employees to enter and exit through the same entry where items brought in and taken out can be screened. In addition, some managers may require items brought in and taken out to be in clear bags or containers.

Finally, the managers of small businesses could use Exit Interviews to obtain ongoing fraud information from all departing employees. Direct supervisors should not conduct these interviews since they may be motivated to intimidate the departing employee. Managers that do conduct exit interviews should receive training on questioning employees about fraudulent activities and how to handle any emerging data. During these interviews, the departing employee should have an opportunity to tell the interviewing manager what they know about fraudulent activities.

LIMITATIONS

This study used a qualitative design to collect data from multiple employee fraud cases. The chosen cases came from employees prosecuted and found guilty of employee fraud. In addition, insufficient information from some of the identified employee fraud forced the exclusion of those cases from the study. Therefore, the results and recommendations associated with this study should not be generalized toward other individuals or groups of small businesses that may suffer from employee fraud.

CONCLUSION

Without a doubt, [small business] managers may place an overwhelming amount of trust in employees (Hrncir & Metts, 2012). While trust in employees is a positive attribute that can enhance working relations, the small business manager must maintain skepticism (Kapp & Heslop, 2011). Skepticism is necessary since employees can develop personal needs, addictions, or vices that motivate them to misappropriate assets. Unfortunately, small businesses often do not have the resources required for a comprehensive set of internal controls. Therefore, small business managers need to identify low-cost methods that can help prevent, detect, or deter fraudulent activities.

REFERENCES

ACFE, (2020). *The 2020 Report to the Nations.* Association of Certified Fraud Examiners. Austin, TX.

Boyle, D.M., Boyle, J.F. & Mahoney, D.P. (2015). "Avoiding the Fraud Mindset." *Strategic Finance,* Volume 97, Number 2, 41-6.

Brody, R. G. (2010). "Beyond the Basic Background Check: Hiring the 'Right' Employees." *Management Research Review*, Volume 33, Number 3, 210-223. doi 10.1108/01409171011030372

Coenen, T. L. (2008), *Essentials of Corporate Fraud.* John Wiley & Sons, Inc., Hoboken, New Jersey.

Dorminey, J.W., Fleming, A.S., Kranacher, M., Riley, R.A. (2010). Beyond the Fraud Triangle. *CPA Journal,* Volume 80, Number 7, 16-23.

Dorminey, J.W., Fleming, A.S., Kranacher, M., Riley, R.A. (2012a). Financial fraud: A New Perspective on an Old Problem. *CPA Journal*, Volume 82, Number 6, 61-65.

Dorminey, J.W., Fleming, A.S., Kranacher, M., &Riley, R.A. (2012b). The Evolution of Fraud Theory. *Issues in Accounting Education*, Volume 2, Number 2, 555-579, doi:10.2308/iace-50131

Groot, W. & van den Brink, H.M. (2010). The Effects of Education on Crime. *Applied Economics*, Volume *42*, Number 3, 279-289, doi:10.1080/00036840701604412

Henry, L. (2016). Fraud Prevention. *Internal Auditor*, Volume 72 Number 2, 17-19.

Hiscox, (2017). The 2017 *Hiscox Embezzlement Study: A Report on White Collar Crime in America*. Retrieved from: https://www.hiscox.com/documents/2017-Hiscox-Embezzlement-Study.pdf

Hrncir, T., &*Metts, S. (2012).* Why Small Business Fall Victim to Fraud: Size and Trust Issues. *Business Studies Journal*, Volume 4, Number 1, 61-71.

Kapp L.A., & Heslop, G. (2011). Protecting Small Businesses from Fraud. *CPA Journal*, Volume 81, Number 10, 62-67.

Katopol, P.F. (2018). The Truth is Out There: Management by Walking Around. Library *Leadership & Management*, Volume 32, Number 4, 1-5.

Klein, R. (2015). How to Avoid or Minimize Fraud Exposures. *CPA Journal*, Volume 85, Number 3, 6-8.

Murdock, H. (2008). The three dimensions of fraud. *Internal Auditor, 65*(4), 81-83.

Nance, J. (2003). *Conquering Deception.* 2nd Edition. Kansas City: Irwin-Benham.

Peltier-Rivest, D., & Lanoue, N. (2012). Thieves from within: Occupational fraud in Canada. Journal of Financial Crime, 19(1), 54-64. doi: 10.1108/13590791211190722

Peterson, B.K. (2003). Fraud Education for Accounting Students. *Journal of Education for Business*, Volume 78, Number 5, 263-267. doi:10.1080/08832320309598612

PwC. (2020). 2020 *Fighting Fraud: A Never-Ending Battle*. PwC's Global Economic Crime and Fraud Survey. Retrieved from: www.pwc.com/fraudsurvey

Ruggieri, L. (2012). From horses to log cabins-A $9 million embezzlement case: How did the owner not know? *Journal of Business Case Studies (Online),* Volume 8, Number 6, 575-584.

Sims, M. (2010). National culture effects on groups evaluating internal control. *Managerial Auditing Journal*, Volume 25, Number 1, 53-78, doi.10.1108/02686901011007306

Ulmer, J.L., & Noe, K. (2013). Embezzlement in the library. *Journal of Business Case Studies (Online),* Volume 9, Number 2, *157-163.*

Journal of Business and Accounting
Vol 14, No 1; Fall 2021

INNOVATIVE BANK MARKET RISK MEASUREMENT STRATEGIES USING A MODERN MACHINE LEARNING APPROACH: A NOVEL AGLOMERATIVE CLUSTERING MODEL ANALYSIS

Karina Kasztelnik
Colorado State University – Global Campus

Abstract

Large Financial Institutions play crucial roles in the content of bank market risk. I present insights into novel and complex issues regarding capital market activities and related bank risk management activities. Previous big-data studies with clustering model analysis have made predictions or measured associations, but not undiscovered data patterns. As such, my agglomerative clustering model approach involving deep machine learning—ultimately to investigate bank market risk both pre- and post-COVID-19 in the United States—is novel and helps uncover trends aligning with Basel II regulations. I derive important perspectives and measurements vis-à-vis bank risk measurement strategy improvements; these may produce positive social changes by enhancing the quality of bank contagion risk measurement worldwide. Overall, these results indicate that a modern machine learning model helps to discover all undiscovered trends supported by Basel II regulations. This modern study contributes to the current literature through its successful use of a novel agglomerative clustering model to derive important perspectives and measurements related to improving innovative bank risk measurement strategies. These findings may produce positive social change by increasing bank contagions risk quality around the World. Finally, the collected data provide relevant information on how empowerment strategies can improve the overall sense of modern bank risk measurement strategies through artificial intelligence.

Keywords: Market Risk, Capital Market, Contagion Bank Risk, Machine Learning

JEL Classifications: C82, E02, G32, D81, F32

INTRODUCTION

Market risk is defined as the risk of loss embedded in all market movements, seen in terms of market price level and volatility. Machine learning allows us to detect meaningful data patterns, and so it has become a tool commonly used to extract

from datasets the most meaningful information. Practitioners are increasingly adopting machine learning alongside other tools and domain knowledge to evaluate complex relationships within datasets. Business data analytics are vital, for deriving effective means of communicating data insights and for deploying business recommendations. There is a need for innovative data-driven concepts that use (and are based on) analytics that identify effective business strategies, in order to increase the efficiency, efficacy, and quality of business decision-making. Previous studies on big-data analytics have not used clustering model analysis to uncover data patterns; rather, they have done so only to make predictions or measure associations. To the best of my knowledge, clustering models have never been used to solve real business problems related to bank market risk (Artzner et al., 1999).

LITERATURE REVIEW

Zhou and Wang (2012) propose the allocation of weight values to decision trees to derive better predictions. They attempted to address the binary classification problem, and their experimental results showed that the algorithm beats the original random forest method in terms of overall accuracy metrics. Galindo and Tamayo (2000) undertook a comparative analysis of statistical and deep machine learning classification techniques to derive accurate predictions of individual-level risk. Khandani et al. (2010), in looking to improve classification rates for credit card holder delinquency and default, constructed a nonlinear, nonparametric forecast model. Yu et al. (2016) proposes a novel multistage deep belief network based on extreme machine learning, as a tool by which to assess credit risk. Wang et al. (2005) propose a new fuzzy support vector machine, while Huang et al. (2007) designed a credit-scoring model to evaluate application credit scores in terms of input features and based on a hybrid support vector machine. Raei et al. (2016) researched a new hybrid model by which to estimate the probability of default of corporate customers in commercial banking; the overall accuracy of this hybrid model indicated it outperformed both base models. Finally, many studies go beyond providing classification-related algorithms (Abraham & Cox, 2007).

Machine learning techniques have been found to perform better than traditional statistical techniques, in terms of both classification and predictive accuracy (Acharya & Richardson, 2009). There appears to be a dearth of literature on deep machine learning models used to assess market risk. Many research studies address market volatility from the management perspective (Ahmed et al., 2006); indeed, there is a conspicuous lack of consideration of market risk measurement from a bank risk management perspective (Engle et al., 2006). Cluster analysis has been undertaken in the medical industry to uncover data patterns (Alexander & Sheedy, 2006), but never in the banking context. Some researchers see clusters as mixtures of multivariate normal populations, where each cluster can be considered a multivariate normal population (Financial Stability Board, 2012). Because each cluster forms a different population, it is possible to conceptualize a "mixture" of populations present in the database, available for sampling. This scenario is a

logical extension of the use of normal distribution in other cases (Barzun & Graff, 1992).

Clustering seeks to identify a finite set of clusters to describe data. In cluster analysis, one partitions similar objects into meaningful classes, when both the number of classes and their composition are to be determined (Brands, 2000). The use of latent class models is frequently seen in the cluster analysis field; these models provide a useful probabilistic/statistical means of grouping observations into clusters (Chernobai et al., 2007). Under this clustering approach, each unique cluster in the population is assumed to be described by a different probability distribution; there is also the understanding that while two clusters may belong to the same family, they may differ in terms of distribution parameter values (Fonseca, 2013).

Artificial intelligence can inform microeconomic decision-making and thus enhance business leadership and management acumen concerning big data and social media analytics (Coetzee & De Beer, 2016). In this way artificial intelligence can further develop the degree to which businesses are set up to gather and clean data; it can also instill trust in automated processes and ensure that decision-making aligns with the organization's strategy, mission, and vision (Abdellaoui & Wakker, 2005). Recent startups find descriptive analytics easy to follow in terms of decision-making, as they relate to overhead, revenue, asset amortization, and liquidity, among other metrics (Brătăşanu, 2017; Bryant, 2014). These data elements work as key financial indicators in developing a real-time understanding of microeconomic applications (De Jongh et al., 2013).

Traditional decision-making models—such as those in finance or marketing—may be considered obsolete, or found difficult to use by managers and leaders as they consider the vastness of the information or data they have at hand; novel analytical techniques could help them pivot their businesses and become more agile in times of uncertainty (Samuel et al., 2018; Song et al., 2019). The burgeoning literature in this area shows a marked willingness to use innovative approaches vis-à-vis predictive analytics that use big data and social media, juxtaposed with various facets of human decision-making and traditional corporate practices (Stephens, 2004). When profits, ethical practices, and related applications are considered, there is a broad array of experiences concerning knowledge acquisition, sharing, and transference at the management or leadership level (Bryant, 2014).

RESEARCH QUESTIONS

The current study poses the following research questions with respect to global systemically important banks (GSIBs), as well as related hypotheses.

RQ 1: Is there a statistically significant relationship between opening and closing stock prices among GSIBs between 2008 and 2020?

H_0: There is no statistically significant relationship between opening and closing stock prices among GSIBs between 2008 and 2020.

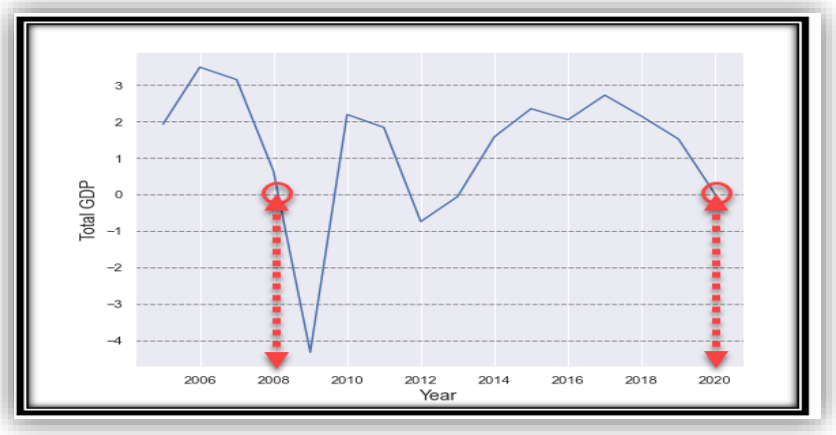
H_1: There is a statistically significant relationship between opening and closing stock prices among GSIBs between 2008 and 2020.

RQ 2: Is there a statistically significant relationship between the adjusted stock price and the volume of stock transactions among GSIBs between 2008 and 2020?
H_0: There is no statistically significant relationship between the adjusted stock price and the volume of stock transactions.
H_1: There is a statistically significant relationship between the adjusted stock price and the volume of stock transactions.

METHODOLOGY: RESEARCH DESIGN AND DATA ANALYSIS PROCESS

Gross domestic product (GDP) is the standard measure of value-added created through the production of goods and services; as such, it measures the fiscal health of a country. I wish to examine the period that features the most fluctuation, and in the GDP graph I selected the same time points (Figure 1). The US GDP in 2008 (i.e., during the subprime crisis) is identical to that achieved in 2020 (i.e., during the COVID-19 pandemic). Additionally, it is noteworthy that the GSIB group market behaved in similar ways before the financial economic recession and before the COVID-19 global pandemic. I want to examine this period to uncover data anomalies that can be interpreted by humans.

Figure 1. US Gross Domestic Product (2006–2020)

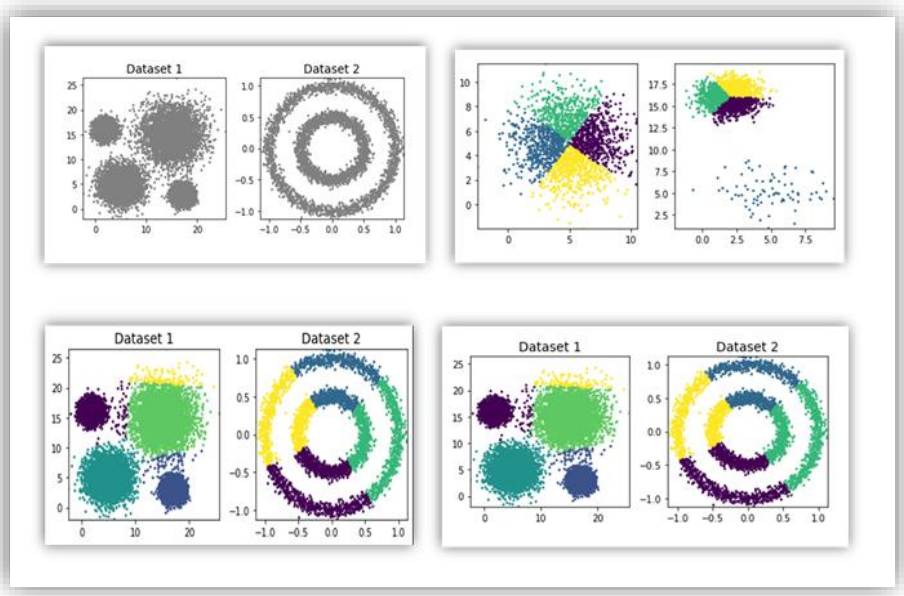


Source: Compiled by the author.

I used nonhierarchical clustering analysis to generate groupings of a sample of elements among the GSIBs, by partitioning the data and producing a smaller set of nonoverlapping clusters that feature no hierarchical relationships (Faul et al., 2007). My starting point was the choice of the number of clusters, *q*. I then grouped the GSIBs on the basis of the minimum distance between them and the seed points. Starting from a classification, GSIBs were iteratively transferred from one cluster

to another (or swapped with banks from other clusters) until no further improvements could be made (Faul et al., 2009). All banks belonging to a given cluster were used to discover a new point that represented the average position of their spatial distribution (Freixas & Laux, 2012). This was done for each cluster CL_K (k = 1,2, …, q), and the resulting points were called the cluster centroids C_K. This process was repeated, and it ended when the new centroids coincided with the old ones. As mentioned, the spatial distribution of the set elements created what is known as a *k*-means graph (Figure 2).

Figure 2. GSIB Dataset Partitioned into Four Clusters and Two Datasets



Source: Compiled by the author.

I used the Silhouette function to define the number of clusters.

$$S_i(q) = \frac{\min\limits_{p,p\neq k}\left[\sum_{l=1}^{N-n_k}\frac{d_{il}}{N-n_k}\right] - \sum_{j=1}^{n_k}\frac{d_{ij}}{n_k}}{\max\left[\sum_{j=1}^{n_k}\frac{d_{ij}}{n_k}, \min\limits_{p,p\neq k}\left[\sum_{l=1}^{N-n_k}\frac{d_{il}}{N-n_k}\right]\right]}$$

, (1)

where the first term of the numerator is the average distance from the *i*-th GSIBs in cluster *k* to

I-th banks placed in a different cluster p (p = 1, …, q), minimized over clusters. The second term is the average distance between the *i*-th banks and another bank *j* placed in the same cluster *k*. $S_i(q)$ is a measure of how similar bank *I* is to others within its own cluster, compared to those in other clusters (Hora, 2016). The range is from –1 to +1; a value near +1 indicates that bank *I* is well matched to its own cluster, and –1 that it is poorly matched to neighboring clusters (Kim et al., 2004).

I ran the model using the Python programming language, from the start to the final visualization. I developed the algorithm by leveraging Panda, NumPy, Matplotlib, Sklearn, and Dash (Nier & Baumann, 2006). I selected the entities to be clustered, and I chose the sample of elements so as to be representative of the cluster structure in the GSIB group population. Second, I selected a number of variables for use in the cluster analysis: opening stock price, closing stock price, adjusted stock price, and volume of stock transactions. These variables provide sufficient information to cluster all my objects (Pastor & Stambaugh, 2001). Next, I standardized the data and selected all similar and dissimilar measurements. I then determined the number of clusters. In my final step of the clustering process, I completed my interpretation, and tested and replicated the resulting cluster analysis. I leveraged my personal banking knowledge and expertise to interpret the clusters within the context of this research study. All completed steps herein are critical steps undertaken in any cluster analysis (Pastor et al., 2007).

Selected Clusters and Additional Data Characteristics:
Dataset 1: Cluster 1: 3870; Cluster 2: 4085; Cluster 3: 4110; Cluster 4: 4047
Dataset 2: Cluster 1: 4000; Cluster 2: 4048; Cluster 3: 4032; Cluster 4: 4032

Converged after 117 iterations
Converged after 53 iterations

True_labels [:5] with Out array ([1,0,2,2,2])

Features [:5] with Out array ([[9.77075874, 3.27621022],
[–9.71349666, 11.27451802],
[–6.91330582, –9.34755911],
[–10.86185913, –10.75063497],
[–8.50038027, –4.54370383]])

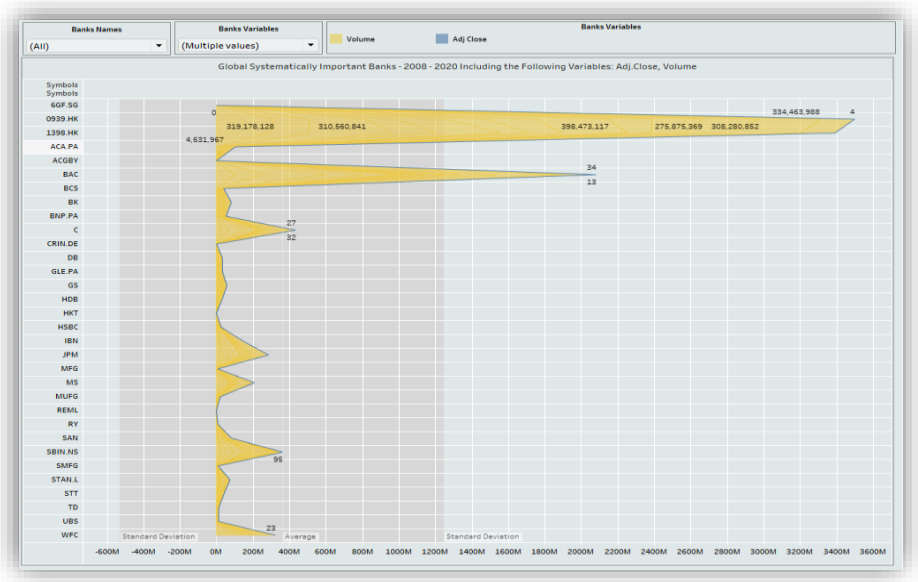
Number of Noise Points Dataset 1: 37(16112)
Number of Noise Points Dataset 2: 38(17514)

RESULTS AND DISCUSSION

I pinpointed data anomalies by leveraging my novel agglomerative clustering model, the features of which underscore the novel nature of the current study. Here, "anomaly detection" refers to finding undiscovered data patterns that do not conform to expected behaviors within the GSIB group (Shadish et al., 2001). At this point, I decided to extend my Python algorithm and use the Dash package to

derive more information about the newly determined data features, to understand the pattern of anomalies. For the sake of accuracy, all anomalies around the selected clusters in datasets 1 and 2 were reconciled with the anomalies in the charts (see Figures 3 and 4).

Figure 3. GSIB Dataset with Individual Features (Adjusted Price, Closing Price, Volume)

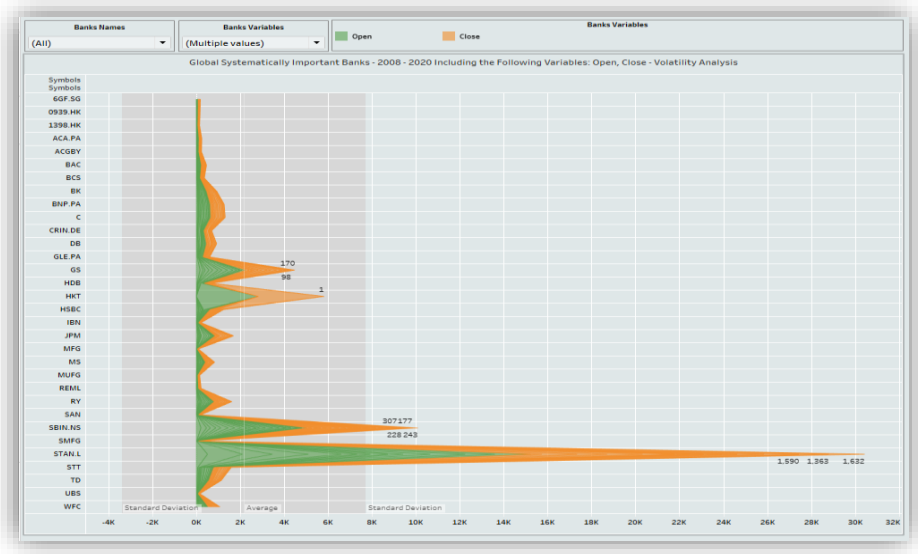


Source: Compiled by the author.

Figure 3 shows that as the volume decreases, any price fluctuations that occur in this area may be less predictable than they were in higher-volume groups. The price action reflects investor sentiment. I confirmed that the stock price by volume shows just how much trust investors have in a dataset trend.

Figure 3 shows the average level (358 M), the top standard deviation (1,249 M), and the bottom standard deviation (–531 M). This information should be considered in light of existing Basel II regulations (i.e., the volume of stock transactions should not exceed the top standard deviation from the current value observed by the GSIB); such actions, when done on a widespread and sustained basis, would help preclude in the short term financial collapse and an unexpected global economic recession (Shenton, 2004). Essentially, I discovered a new threshold by which to assess new contagion bank market risk, and my dashboard is a fully interactive tool that can be used in daily bank operations to track such anomalies in the GSIB data (Basel Committee on Banking Supervision, 2011).

Figure 4. A GSIB Dataset with Individual Features (Opening Price, Closing Price, Volatility)



Source: Compiled by the author.

Figure 4 shows the average level (2,169 K), the top standard deviation (7,710 K), and the bottom standard deviation (–3,375 K). Again, this information should considered in light of existing Basel II regulations (i.e., closing stock prices should not exceed the top standard deviation from the current value observed by the GSIB); doing so would likewise help preclude in the short term an economic recession.

GRAPH: OPENING–CLOSING STOCK PRICES

Note in Figure 4 that the Goldman Sachs Group (GS) shows high volatility within the GSIB group. This means a security's value can be potentially spread over a larger range of values, and that the stock price can change dramatically over a short period, in either direction. The State Bank of India (SBIN.NS) shows a high level of volatility and exceeds the graph's healthy standard deviation. Among all the GSIBs, Morgan Stanley (STAN.L) shows the highest volatility. This individual open interest numbers in the stocks do provide valuable information. They tell us which contracts are the most liquid, for observation purposes. As a general rule, trading activity should be limited to those delivered monthly, and annually for those with the highest open interest.

GRAPH: VOLUME OF STOCK TRANSACTIONS

In the current study, a stock's trade volume is the total number of shares traded between 2008 and 2020. In Figure 3, one sees that ING Bank Slask (6GF-SG) and Credit Agricole S.A. (ACA.PA) each lost a considerable amount of stock trade volume between these two years. Meanwhile, the China Construction Bank Corporation (0939.HK) and Industrial and Commercial Bank of China Limited

(1398.HK) gained in terms of stock trade volume. At the same time, I found that some banks—such as Deutsche Bank Aktiengesellshaft (DB), Société Générale (GLE.PA), The Goldman Sachs Group, Inc. (GS), HDFC Bank Limited (HDB), and Hong Kong Trust (HKT)—showed very low stock volumes; this means they were less actively traded during the study period. I also found that when stocks start to trade irregularly at low volumes, it signals problems with volatility, market uncertainty, and liquidity risk. The concept of a trend is absolutely essential to taking a technical approach to risk market analysis: in a general sense, trends are simply market directions, but to work with my deep machine learning model, a more precise definition and observation are needed. Volume plays an important confirming role in all of these price patterns. In times of doubt, a study of earlier volume patterns accompanying price data can be a deciding factor as to whether or not the pattern can be trusted (Shenton, 2004). Additionally, most price patterns can be used with certain statistical measurement techniques that can help digital analysts determine minimum price objectives; these are helpful in assisting traders in determining their reward–risk ratio. The results herein show more deeply how the proposed machine learning solution can extend risk measurement practices currently used worldwide.

CONCLUSION AND RECOMMENDATIONS

The current study proposed a novel agglomerative clustering model; the analytical results indicate it can improve bank market risk measurement by uncovering data trends that, when leveraged, can lead to bank policy improvements that align with Basel II. The current study also identified essential anomalies in data from global systemically important banks, as strong new contagion market risk ratios; these can support meaningful analysis among operational researchers. In the absence of novel agglomerative clustering model analysis, it would be quite difficult and time-consuming to pinpoint patterns in real, nonhistorical data. There is a need for new digital research or digital data science approaches that feature strong domain knowledge, in tandem with advanced technology, to support bank executives and leaders in financial institution industries. The results herein indicate that artificial-intelligence–driven solutions can guide humans in pinpointing “red flags” and reacting quickly so as to preclude extensive damage to the worldwide economy.

Business data analytics are vital to both effectively communicating data insights and deploying business recommendations. If the efficiency, effectiveness, and quality of business decision-making is to be enhanced, the development of innovative data-driven concepts that use (and are based on) analytics is essential, to identify effective banking risk strategies. The research results presented herein confirm that the proposed agglomerative clustering model and concomitant human domain knowledge interpretations can support public or private bank leaders as they work to discover and better understand essential bank market risk anomalies as a part of modern behavioral prescriptive analytics. For this reason, the current study should be of value to bank practitioners who wish to derive higher-quality current risk market measurement data insights and better inform their financial business strategy decisions. Using the same research design and analysis, future

research could investigate other US industries or other available and measurable risks to uncover previously unknown data trends.

REFERENCES

Abdellaoui, M., & Wakker, P. P. (2005). The likelihood method for decision under uncertainty. *Theory and Decision, 58(1), 3–76.* https://doi.org/10.1007/s11238-005-8320-4

Abraham, S., and P. Cox. 2007. Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *The British Accounting Review* 39(3): 227–248. https://doi.org/10.1016/j.bar.2007.06.002

Acharya, V, Richardson, M, (2009) "Restoring Financial Stability –How to Repair a Failed System", *John Wiley & Sons, p, 1-418*, https://doi.org/10.1016/S2212-5671(15)01516-6

Ahmed, A.S., E. Kilic, and G.J. Lobo. 2006. Does recognition versus disclosure matter? Evidence from value-relevance of bank's recognized and disclosed derivate financial instruments. *The Accounting Review* 81(3): 567–588. https://doi.org/10.2308/accr.2006.81.3.567

Alexander, C, Sheedy, E, (2008) "Developing a stress testing framework based on market risk models", *Journal of Banking and Finance, 32, p,2220-2236* https://doi.org/10.1016/j.jbankfin.2007.12.041

Artzner, P, F, Delbaen, J. Eber, J, Heath, D, (1999) "Coherent measures of risk", *Mathematical Finance, p,203-228* https://people.math.ethz.ch/~delbaen/ftp/preprints/CoherentMF.pdf

Basel Committee on Banking Supervision, (2011) "Messages from the academic literature on risk measurement for the trading book", *Bank for International Settlements Communications, Working paper no, 19* https://www.bis.org/publ/bcbs_wp14.pdf

Barzun, J., & Graff, H.F. (1992). The modern researcher: A classic work on research and writing completely revised and brought up to date. *Harcourt Brace Jovanovich.*

BRĂTĂŞANU, V. (2017). Digital innovation the new paradigm for financial services industry. *Theoretical & Applied Economics, 24, 83–94.* https://ideas.repec.org/a/agr/journl/vxxivy2017ispecialp83-94.html

Bryant, W. D. A. (2014). The Microeconomics of Choice under Risk and Uncertainty: Where Are We? Vikalpa: *The Journal for Decision Makers, 39(1), 21–40.*

Brands, H. W. (2000). The first American: The life and times of Benjamin Franklin.
Doubleday https://doi.org/10.2307/2700631
Chernobai, A. S., Rachev, S. T., & Fabozzi, F. J. (2007). Operational risk: A guide to Basel II
capital requirements, models, and analysis. *New Jersey: John Wiley*.
Coetzee, J, & De Beer, J. (2016). Financial regulation in the south African banking industry. In (Ed.), *Bank risk management in south Africa - a risk-based perspective*. Cape Town:
Juta. https://doi.org/10.1108/AJEMS-08-2019-0316
De Jongh, E., De Jongh, D., De Jongh, R., & Van Vuuren, G. (2013). A review of operational
risk in banks and its role in the financial crisis. *South African Journal of Economic*
and Management Sciences, 16(4), 364–382. doi:10.4102/sajems. v16i4.44
https://doi.org/10.4102/sajems.v16i4.440
Engle, R. F., E. Ghysels, and B. Sohn. (2006). On the Economic Sources of Stock
Market Volatility, University of North Carolina at Chapel Hill, Manuscript.
Financial Stability Board. 2012. *Enhancing the risk disclosures of banks*. Basel.
Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*, 175-191. https://doi.org/10.3758/BF03193146
Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*, 1149-1160. https://doi.org/10.3758/BRM.41.4.1149
Freixas, X., and C. Laux. 2012. Disclosure, transparency, and market discipline. In *The crisis*
aftermath: New regulatory paradigms, ed. M. Dewatripont and X. Freixas, 69–104.
London: Centre for Economic Policy Research.
https://voxeu.org/article/market-discipline-disclosure-and-transparency
Galindo, Jorge, and Pablo Tamayo. 2000. Credit Risk Assessment Using Statistical
and Machine Learning: *Basic Methodology and Risk Modeling Applications. Computational Economics15: 107–43*
https://doi.org/10.1023/A:1008699112516
Hora, M. T. (2016). Navigating the Problem Space of Academic Work: How Workload and Curricular Affordances Shape *STEM Faculty Decisions About Teaching and Learning. AERA*
Open. https://doi.org/10.1177/2332858415627612

Huang, Cheng Lung, Mu Chen Chen, and Chieh Jen Wang. 2007. Credit Scoring with a Data Mining Approach Based on Support Vector Machines. *Expert Systems with Applications33: 847–56* https://doi.org/10.1016/j.eswa.2006.07.007

Jaime R.S. Fonseca (2013) Clustering in the field of social sciences: that is your choice, *International Journal of Social Research Methodology, 16:5, 403-428,* https://doi.org/10.1080/13645579.2012.716973

Khandani, Amir E., Adlar J. Kim, and Andrew W. Lo. 2010. Consumer credit-risk models via machine-learning algorithms. *Journal of Banking & Finance34: 2767–87.* http://hdl.handle.net/1721.1/66301

Kim, C.-J., J. C. Morley, and C. R. Nelson. (2004). *''Is there a Positive Relationship Between Stock Market Volatility and the Equity Premium?* http://research.economics.unsw.edu.au/jmorley/kmn04.pdf

Nier, E., and U. Baumann. 2006. Market discipline, disclosure and moral hazard in banking. *Journal of Financial Intermediation* 15(3): 332–361. https://doi.org/10.1016/j.jfi.2006.03.001

Pastor, L., and R. F. Stambaugh. (2001). ''The Equity Premium and Structural Breaks. *''Journal of Finance 4, 1207 – 1231.* https://doi.org/10.1111/0022-1082.00365

Pastor, L., M. Sinha, and B. Swaminathan. (2007). ''Estimating the Intertemporal Risk – Return Tradeoff using the Implied Cost of Capital.'' *Forthcoming in Journal of Finance.* http://dx.doi.org/10.2139/ssrn.878685

Raei, Reza, Mahdi Saeidi Kousha, Saeid Fallahpour, and Mohammad Fadaeinejad. 2016. A Hybrid Model for Estimating the Probability of Default of Corporate Customers. *Iranian Journal of Management Studies9:651–73.* http://doi.org/10.22059/ijms.2016.57714

Samuel, J., Kashyap, R., & Kretinin, A. (2018). Going Where the Tweets Get Moving! An Explorative Analysis of Tweets Sentiments in the Stock Market. Proceedings of the *Northeast Business & Economics Association, 281–285.* https://doi.org/10.1016/j.heliyon.2021.e06200

Song, T., Huang, J., Tan, Y., & Yu, Y. (2019). Using User- and Marketer-Generated Content for Box Office Revenue Prediction: Differences between Microblogging and Third-Party Platforms. *Information Systems Research, 30(1), 191–203.* https://doi.org/10.1287/isre.2018.0797

Shadish, W., Cook, T., & Campbell, D. (2001). *Experimental and quasi-experimental designs for generalized causal inference*. *Houghton Mifflin.*

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information, 22*, 63-75. http://doi.org/10.3233/EFI-2004-22201

Stephens, L. J. (2004). *Advanced statistics demystified*. McGraw-Hill.

Wang, Yongqiao, Shouyang Wang, and Kin Keung Lai. 2005. A New Fuzzy Support Vector Machine to Evaluate Credit Risk IEEE *Transactions on Fuzzy Systems13: 820–31* *http://doi.org/* 10.1109/TFUZZ.2005.859320.

Yu, Lean, Zebin Yang, and Ling Tang. 2016. A Novel Multistage Deep Belief Network Based Extreme Learning Machine Ensemble Learning Paradigm for Credit Risk Assessment. *Flexible Services and Manufacturing Journal28: 576–92*. https://doi.org/10.1007/s10696-015-9226-2

Zhou, Lifeng, and Hong Wang. 2012. Loan Default Prediction on Large Imbalanced Data Using Random Forests. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* https://doi.org/10.11591/TELKOMNIKA.V10I6.1323

Journal of Business and Accounting
Vol 14, No 1; Fall 2021

HIGH SPEED RAIL, IMMINENT DOMAIN AND PROPERTY RIGHTS – THE SAGA CONTINUES

Christopher Thompson
Hope Knight
Laura Sullivan
Sam Houston State University

ABSTRACT

Dallas and Houston are merely 90 minutes apart and a significant number of people commute between the two cities in heavy traffic. With a goal to reducing the travel time and allowing commuters to begin their day with a review of what will come when they arrive at work, Texas Central Partners, LLC proposed the development of a high-speed rail between the cities. However, it soon turned out that the proposition conflicted with property rights an imminent domain issues. The purpose of this paper is to analyze the proposition of Texas Central Partners in relation to imminent domain and property rights.

Key Words: Property rights, eminent domain, Federal and State Constitutions, Delegation of Powers.

INTRODUCTION

In 2009, Lone Star High Speed Rail, LLC, the predecessor of Texas Central was formed. Then in 2012, Texas Central Railroad Partners, Inc. and Texas Central Partners, LLC (collectively referred to as Texas Central) were formed in 2010 (Martin). Texas Central Railroad Partners' role is to develop the line and Texas Central Railway's role is to advocate for building the line. Their stated purpose is to build a wholly private rail line connecting Dallas and Houston with high speed bullet trains, making the 240 mile trip with trains departing every half hour during peak travel times and making a single stop along the way near Roan's Prairie, in Grimes County (The Project). The company's ability to do so is dependent upon whether it has the right to condemn property belonging to unwilling property owners along the route using eminent domain.

The power of eminent domain is inherent in the sovereign powers of both the Federal and Texas Constitutions, however both the State and Federal

governments may delegate their power to private entities. In Texas, these delegates include (among others) cities, towns, colleges, school districts, pipeline companies, utility companies and railroads (Leopold).

Legally speaking, the issue turns on the meaning of the phrase "operating a railroad" as used in the Texas Transportation Code. If Texas Central is "operating a railroad", it enjoys the full power of eminent domain equivalent to that of the State itself. However, if it is merely an entity formed in the hope of operating a railroad in the future, it has no eminent domain power whatsoever. In this framework, it is no surprise that Texas Central takes the position that its current day-to-day activities, as it prepares to construct and operate a rail line, constitutes "operating a railway." Equally apparent should be the opposition's position that "operating a railroad" requires a currently existing railway with trains running on it.

The exercise of eminent domain is rarely a popular topic but is even less popular in a state like Texas which maintains strong ties to its agrarian past and present. Texas Central's plan is exceptionally unpopular among the communities that lie along its proposed route for several reasons. The possibility that anyone could form a business on Monday with the intention to operate a railway, and on Tuesday begin the eminent domain process to take private property is an unsettling prospect. This is only amplified by the fact that over ninety-five (95) percent of the real property in the Texas is privately owned (Lopez, et., al). This is not the only aspect of Texas Central's Plan that its detractors and opponents find concerning.

First, Texas Central is a business entity backed (or is at least alleged to be backed) by international business interests. Second, the company has acknowledged that it lacks the funding to carry the project to completion. Finally, no matter how convenient it is for people traveling between Houston and Dallas, the planned line only has one stop in between located in remote Roan's Prairie. As a direct consequence, a majority of landowners whose land would be burdened by the railway, as well as the communities along the route, cannot make any practical use of it.

There is a great deal at stake for all parties involved in this struggle. Texas Central has associated and or retained a retired Texas Supreme Court Justice who has added his voice to the mix by essentially rendering his own advisory opinion on the matter (Enoch). Landowners along the proposed route are to a large degree represented by Texans Against High Speed Rail, a non-profit corporation devoted to "defeating" Texas Central.

To date two challenges to Texas Central's self-proclaimed imminent domain powers have been litigated to a conclusion at the trial court level. One in Harris County resulted in a win for Texas Central, but only because the landowner failed to follow through with their suit resulting in a default

judgment. The second, and far more important case, involved a challenge in Leon County resulting in a defeat for Texas Central in the form of a judicial ruling that the company is not "operating a railroad" and thus has no powers of imminent domain (Matthews).

ABOUT TEXAS CENTRAL RAILWAY'S PLAN

Texas Central's plan is to connect Dallas and Houston by high-speed rail, reducing a one-way trip down to ninety (90) minutes using train technology already being used in other countries (Safety and Security). Texas Central has doggedly asserted that it will accomplish this feat without a drop of public funding despite an estimated cost of more than twelve (12) billion dollars (Learn The Facts).

The technology portion of Texas Central's plan appears sound. It has partnered with Central Japanese Railway (CJR), the company responsible for the technology utilized by the Shinkansen bullet train system in Japan. The Shinkansen has operated since 1964 and has never suffered a wreck or crash resulting in passenger injury or fatality (Learn The Facts). The trains themselves are not the source of much concern. What concerns many critics is the role CJR and the Japanese Bank for International Cooperation will have in the operation of Texas Central should the rail-line actually get built. To date, Texas Central's largest source of financing is a $300 million loan backed by Japanese interests announced in late 2018. This loan dwarfs the roughly $75 million in capital raised by Texas Central from private investors. Among those Japanese interests is the state-owned Bank of International Cooperation (JBIC). JBIC describes itself as a "policy-based financial institution" with four goals:

1) Promoting the overseas development and securement of resources which are important for Japan;
2) Maintaining and improving the international competitiveness of Japanese industries;
3) Promoting the overseas business having the purpose of preserving the global environment; and
4) Preventing disruptions to international financial order or taking appropriate measures with respect to damages caused by such disruptions (Japan Bank for International Cooperation).

Goal number two (2) is where Texas Central comes in. Pursuant to this goal, JBIC provides financing to buyers of Japanese machinery for infrastructure projects outside of Japan (Japan Bank for International Cooperation).

The question hovering over JBIC's massive loan to Texas Central is whether it was made because the bank believes in Texas Central's project or if it was made just to create a market for CJR's trains.

THE EMINENT DOMAIN PROCESS IN TEXAS

Eminent domain is the power of the government to take private property belonging to citizens for public use. Both the United States and Texas Constitutions limit this power and require payment of adequate compensation to the party suffering the taking (The Texas Constitution, Article 1, § 17). When an entity actually uses its power of eminent domain it is commonly referred to as condemnation.

The exercise of eminent domain in Texas is controlled by Title 4, Chapter 21 of the Texas Property Code. The code lays out a rather straightforward standard procedure applicable in all cases (Texas Property Code Title 4, Section 21.011). The process itself is not complicated.

First, the entity (assuming it has eminent domain authority) attempting to acquire real property must make a "bona fide offer" to purchase the property at private sale (Texas Property Code Title 4, Section 21.013). An offer is "bona fide" if it meets certain statutory requirements. These include: 1) an opening offer made in writing, 2) a written appraisal from a certified appraiser of the property's value and any damages to the owner's remaining property, 3) followed by a final offer made in writing at least thirty (30) days after the opening offer was made. Said final offer must be equal to or in excessive of the appraisal and allow the property owner at least fourteen (14) days to make a decision (Texas Property Code Title 4, Section 21.013 (b)).

Second, if the parties cannot reach an agreement the entity seeking to acquire the property may begin condemnation proceedings by filing a petition in either the state judicial district court or county court at law (Texas Property Code Title 4, Section 21.001). However, district courts are empowered to decide any issue relating to a condemnation case, including whether the entity seeking to exercise eminent domain has the authority to do so in any suit involving a claim for property, damages to property occupied under eminent domain, or for an injunction to prevent a party from entering or using the property under eminent domain (Texas Property Code Title 4, Section 21.003). Venue in a condemnation case is proper in the county where the property owner resides if they live in any county where the property at issue is located or in any county where part of the property is located if the owner does not reside in a county the property is located in (Texas Property Code Title 4, Section 21.013 (a)).

Finally, the presiding court must appoint three (3) special commissioners who are disinterested real property owners residing in the county for the purpose of assessing the damages that will be suffered by the property owner when condemnation is complete. These special commissioners are tasked with assessing the amount. of damages fairly and impartially and are armed with the power to compel witnesses, punish contempt, and administer oaths (Texas Property Code Title 4, Section 21.014). The special commissioners must hold a hearing, calculate the damages that will be suffered, and file their findings with the presiding court. If no party files a timely objection to the commissioner's findings, the court will adopt those findings as the court's judgment and issue any process necessary to see the judgment enforced (Texas Property Code Title 4, Section 21.061). If any party does lodge a timely objection then the case proceeds to trial and is treated like any other civil cause of action (Texas Property Code Title 4, Section 21.018). It is only at this stage that a landowner resisting condemnation may actually raise some very important issues, namely whether the entity attempting to condemn their property has the right to do so and whether the use the property is intended for is truly a "public use (Texas Property Code Title 4, Section 21.003; Dowel)."

PUBLIC USE

Both the Texas Constitution and the United States Constitution limit the exercise of eminent domain to situations when the property taken shall be for public use. However, public use is defined very loosely.

Federally, "public use" has been defined by the U.S. Supreme Court so broadly that even the taking of private property for the purpose of economic development is allowable even when the developed or re-developed property is not open to the public. Essentially, the only limits on "public use" recognized by the Supreme Court are in the following situations. First, a purely private taking, the taking of an owner's property purely for the benefit of another private party would not pass Constitutional scrutiny. Second, a taking merely covered by the pretext of a public purpose but done with the intent to benefit a private party would also not satisfy the public use requirement (*Kelo v. City of New London*, 545 U.S. 469). Any doubt about the breadth of the full extent of the concept under federal law should have died with the Supreme Court's now infamous opinion in *Kelo v. The City of New London.*

In *Kelo*, the Court held that a plan by the city of New London, Connecticut to take the real property owned by individuals in a particular area of town and transfer it to private parties who would then build tax money generating

improvements such as hotels, restraints, offices, and newer, more expensive homes, satisfied the public use requirement, allowing the exercise of eminent domain. The Court was not particularly bothered that huge portions of this ninety acre development would never be made open to the public. The development was intended to create jobs and raise the property tax base by "endeavoring to coordinate a variety of commercial, residential, and recreational uses of land, with the hope that they will form a whole greater than the sum of its parts" and as such is for a public use (*Kelo v. City of New London*, 545 U.S. 469).

The Supreme Court's *Kelo* opinion left no doubt that any private citizen's property could be taken via eminent domain and given to another private entity under the guise of economic development. The effect of this decision reverberates in the Texas Central situation because there is no Constitutional barrier between the wholly privately owned company exercising eminent domain powers, leaving the statutory construction of the Texas Transportation Code as the only impediment to the project's progress.

ENTITIES WITH EMINENT DOMAIN POWERS IN TEXAS

Among the entities to whom the power of eminent domain has been delegated to by the Texas legislature are railroad companies. However, the exact wording of the statute giving railroads this power is at the heart of the current struggle between Texas Central and landowners.

The Texas Transportation Code grants eminent domain powers to all railroad companies incorporated before September 1, 2007, and all other legal entities *operating a railroad*, as well as interurban electric railways (Texas Transportation Code § 112.002 & 131.011-.012). However, the statute referring to interurban railroads refers back to the "rights and powers granted to a railroad company."

Texas Central was not formed until 2010 meaning that if it has eminent domain powers, it is because it is *operating a railroad*. Whether Texas Central meets the *operating a railroad* requirement has been the focus of both of the challenges to Texas Central's agenda in the courtroom.

STATUTORY CONSTRUCTION

Statutory construction is at best an adventure in Texas and at its worst a family vacation to Hell and parts unknown. Every court's goal in the statutory construction realm is to discern the legislative intent behind the statute's adoption. Courts have several tools available to assist them. These

tools include the traditional canons of construction and two statutory schemes for construction. However, it is vital to understand that none of these tools are mandatory or in any way force a particular court to use a particular method to reach its decision (Beal).

Ground zero for any statutory construction puzzle begins with the words themselves (*Boykin v. State*, 818 S.W.2d 782). This is "because our state constitution assigns the law *making* function to the Legislature while assigning the law *interpreting* function to the Judiciary." (*Boykin v. State*, 818 S.W.2d 785) Beginning with the actual wording of the statute being construed is also done out of respect for the process whereby those words became the law and in recognition that the legislators are entitled to having courts that follow the laws as they were written (*Boykin v. State*, 818 S.W.2d 785). As a result, when the literal text of a statute is clear and free from ambiguity, courts give its literal meaning effect (*Smith v. State*, 789 S.W.2d 590, 592). Stated another way, when a statute is understandable and unambiguous, the Legislature should be given the benefit of the doubt that it knew what it was doing when the statute was adopted. Accordingly, when a statute is clear and unambiguous, a court has no business making alterations to it (*Coit. v. State*, 808 S.W.2d 473, 475; *Ex Parte Davis*, 412 S.W. 2d 46, 52). These extends to the canons themselves: "if a statute is unambiguous, rules of construction or other extrinsic aids cannot be used to create ambiguity." (*Fitzgerald v. Advanced Spine*, 996 S.W.2d 864, 866).

As noted above, statutory construction can be an adventure, which is mainly due to the many contradictions between the various canons of construction. The common-law canons include: a presumption that the legislature intended for its words to be given their ordinary meaning; a requirement that a statute be construed as a whole and not considered piece-meal; a presumption that the legislature intended the statute to read as-written, i.e. a "court should not read a word, phrase, or sentence to be useless or a nullity." (Beal). Muddying the waters further are the Code Construction Act and Construction of Laws Act (Tex.Gov.Code § 311, 312). These acts are surely some of the strangest to ever come out of Austin. They are rules allegedly codifying how a statutory construction inquiry should be conducted but in reality have been determined to be merely guidelines with no more power than the traditional canons described above (*Thiel v. Harris County Democratic Exec. Comm.*, 534 S.W.2d 891, 894). Among these statutory canons is section 311.012, stating that construing a statute requires a court to read words in the present or past tenses to also include the future tense (Tex.Gov.Code § 311.012).

Section 311.012 is at the heart of Texas Central's argument that it acquired all of the powers of imminent domain when it was formed because

"operating a railroad" in the Transportation Code includes the intention to operate a railroad at some point in the future *See Defendant and Intervenor's Motion for Partial Summary Judgment*.). Interestingly enough, the Supreme Court of Texas has set some interesting statutory construction precedents related solely to eminent domain cases. Over sixty (60) years ago the Court held that

> The protection which the law has erected for the benefit of the citizen as against the power of the exercise of the power of condemnation should be liberally construed. Stated otherwise, the power of eminent domain must be strictly construed against those corporations and arms of the State vested therewith (*Coastal Gas States Producing v. J. E Pate, et* al, 309 S.W.2d 828, 831).

As recently as 2012, the Supreme Court reiterated this position on construing statutes related to eminent domain and appears to have even extended it by stating that when there are any doubts as to the scope of an entity's statutorily granted eminent domain powers those doubts must be construed in the landowner's favor (*Texas Rice Land Partners, LTD. V. Denbury Green Pipeline-Texas, LLC*, 363 S.W.3d 192, 198).

HARRIS COUNTY CASE

To be clear, more than one case in Harris County (and in other counties, especially Ellis County) has involved Texas Central and the question of eminent domain, however, to date, only one of those has ended with a ruling rendered by the presiding court.

Texas Central sued August S. Lander, a Harris County landowner, in the 334th District Court of Harris County seeking access to his property to conduct surveys and conduct other inspections or examinations related to making routing decisions for Texas Central's project. On January 10th, 2017, Judge Steven Kirkland signed default judgment in favor of Texas Central when the defendant, Lander, did not appear in court. Judge Kirkland's judgment stated that Texas Central was a railroad company with the powers of eminent domain (Martin).

However, this judgment, although a victory, is practically worthless in terms of precedential value because of its default nature.

LEON COUNTY CASE

87th Judicial District Court

In February 2019, State District Judge Deborah Oakes Evans presiding over the 87th District Court of Leon County ruled that Texas Central was not empowered to use eminent domain because it is not "operating a railroad" and is not an "interurban electric railway (Staff, Begley)."

The case began when Leon County landowners James and Barbara Miles resisted Texas Central's demand for access to their property in order to survey the land for its potential acquisition and use for the project. With James as the named plaintiff, they sued Texas Central seeking a declaratory judgment from the court that Texas Central does not have eminent domain powers because it is not operating a railroad. Eventually, Texas Central filed a motion for summary judgment (followed by an amended motion) requesting the court find that there was no genuine issue of fact as to whether it was indeed operating a railroad as contemplated by the Transportation Code. In essence, Texas Central sought a declaration that it is operating a railroad. In its motion as well as its summary judgment evidence, Texas Central conceded that it did not own any locomotives, passenger cars, any depots, or even any tracks (*Defendant and Intervenor's Amended Motion for Summary Judgment" at page 15*). Texas Central's arguments were rooted in the Code Construction Act's section regarding word tenses, and that accordingly, it was "crystal clear" that it is actively operating a railroad *(Defendant and Intervenor's Amended Motion for Summary Judgment" at page 15).*

The Miles' counsel pointed out, in their response to Texas Central's Amended Motion for Summary Judgment, that Texas Central's premise that it acquired eminent domain powers and the right to condemn private property just by incorporating with the intent to operate a railroad one day is very chilling to property owners (*Defendant and Intervenor's Amended Motion for Summary Judgment" at page 15).*

Judge Evans disagreed with Texas Central's position and issued a short ruling that Texas Central was neither operating a railroad nor an interurban electric railway. When one solely relies on the Code Construction Act, it might seem an illogical decision. However, when viewed through the larger lenses of the common law canons of statutory construction, the statutory canons, and the rules of construction unique to eminent domain statutes, it is easier to both appreciate the monumental task the judge was tasked with, as well as how she reached her decision.

Judge Evans' ruling is not effective only in Leon County. The 87th Judicial District also includes Freestone and Limestone Counties, each of which lies

along the planned route for Texas Central's project. Very roughly speaking, one-fourth of the planned 240-mile route was effectively rendered a no-eminent domain zone by Judge Evans' ruling (The Texas Bullet Train).

13th Court of Appeals

As predicted, Texas Central appealed the trial court's decision, contending that Judge Evans erred when she declared that Texas Central was not a railroad company or an interurban electric railway.

The standard of review for a trial court's summary judgment ruling is de novo. *See* Mann Frankfort Stein & Lipp Advisors, Inc. v. Fielding, 289 S.W.3d 844, 848 (Tex. 2009).

Since the parties filed competing motions for summary judgment and the judge granted one and denied the other, the court of appeals reviewed both parties' summary judgment evidence and determined all questions presented. (Valence Operating Co. v Dorsett, 164 S.W.3d 656, 661 (Tex. 2005). Hence, the appellate court had to determine whether Judge Evans properly granted Miles's declaratory judgment requests, and if not, enter the proper judgment.

Texas Central argued that the trial court erred in ruling that Texas Central is not a railroad company as defined in the Texas Transportation Code. *See* Tex. Transp. Code Ann. §81.002. Section 81.002 defines a railroad company as:

(1) A railroad incorporated before September 1, 2007, under former Title 112, Revised Statutes; or

(2) Any other legal entity operating a railroad, including an entity organized under the Texas Business Corporation Act or the Texas Corporation Law provisions of the Business Organizations Code. *Id.*

Texas Central was not incorporated before September 1, 2007, so the Court was left to decide if it is a railroad company under §81.002(2).

Texas Central argued that it was clearly a railroad because it was engaging in railroad operations regulated under Title 5 of the Transportation Code. They argued that while they have not yet physically laid tracks or began to carry passengers or freight onboard trains, they have taken many of the necessary steps to be able to create and operate a railroad in the future.

As noted above, the Supreme Court of Texas has set statutory construction precedent related solely to eminent domain cases and Texas Central relied on the *Texas Rice II* case for the contention that they have eminent domain power. Specifically, Texas Central contends that they qualify as an entity with eminent domain power because they will have trains running on tracks when construction is complete.

Miles argued that "the Legislature chose to use the word "operating" to codify its intent that an entity must demonstrate that it is presently operating

a railroad…" As evidence, Miles stated that Texas Central "owns no trains, have constructed no track or train depots, have expended less than 1% of the total estimated cost of the Project, and cannot even purchase the parcels optioned along the Project's proposed alignment."

As pointed out earlier, every court's goal in statutory construction is to discern the Legislature's intent behind the statute's adoption. In the opinion, the court pointed out that the Legislature's intent should be "ascertained from the plain meaning of the words used in the statute." Sw. Royalties, Inc. v. Hegar, 500 S.W.3d 400, 404 (Tex. 2016); *see also* Combs v. Roark Amusement & Vending, L.P., 422 S.W.3d 632, 635 (Tex. 2013).

Further, the court cited the section in the Code Construction Act that says, "words in the present tense include the future tense." Tex. Gov/t Code Ann. § 311.012(a). The court further noted that Miles would have them ignore the Legislature's instruction under the Code Construction Act by limiting the word "operating" to solely the present tense and declined to do so.

In Texas Rice II, the Texas Supreme Court found a pipeline company was a common carrier under the Texas Natural Resources Code because there was a reasonable probability that the pipeline, "at some point after construction" would "serve the public." *See* Texas Rice II, 510 S.W.3d 909,914. The court found that a pipeline owner must do more than just state that it is a common carrier by filling out the necessary forms to gain eminent domain power, it must also show that it will meet the requirements as set forth in the code. *Id.* At 915-916 (citing Texas Rice I, 363 S.W.3d at 202). The court did not require a showing that it was currently operating in such a way to serve the public, only that there was a reasonable probability that it would in the future. Id.

In the present case, the court discounted Miles' contention that Texas Central has only spent 1% of the overall budget and found that Texas Central had coordinated with regulatory agencies concerning the Project, begun design, construction and management operations, conducted land surveys and entered into purchase agreements.

Ultimately, the Court ruled that Texas Central is a railroad company pursuant to §81.002(2). In its decision, the court cited the Code Construction Act instruction to view present tense as including future tense in the statute and found that Texas Central had taken action to begin to operate a railroad. The court also found that Texas Central was an interurban electric railway.

The Supreme Court of Texas

On June 18, 2021, the Supreme Court of Texas denied the review of the appellate court ruling filed by Miles. Miles has since filed a motion for

rehearing, followed by numerous amicus curiae letters from landowners and companies.

FUTURE AND CONCLUSION

With so much on the line for both sides, this struggle over the meaning of "operating a railroad" is not over. Both sides have vowed to continue the struggle and see it through to the end. Eventually, the case might make its way to the United States Supreme Court.

With so much at stake for Texas Central and its investors, as well as the potential danger to every Texan's private property rights this issue will bear watching over the coming years.

REFERENCES

Beal, R. (n.d.). The Art of Statutory Construction: Texas Style. *Baylor Law Review*.

Begley, D. (2019, February 13). Opponents of Houston-Dallas bullet train trumpet ruling that company is not a railroad. Retrieved from https://www.chron.com/news/transportation/article/Opponents-of-Houston-Dallas-bullet-train-trumpet-13607501.php.

Boykin v. State. (n.d.). Retrieved from https://law.justia.com/cases/texas/court-of-criminal-appeals/1991/1539-89-4.html.

Coit v. State. (n.d.). Retrieved from https://law.justia.com/cases/texas/court-of-criminal-appeals/1991/529-87-4.html.

Coastal States Gas Producing Company v. Pate. (n.d.). Retrieved from https://law.justia.com/cases/texas/supreme-court/1958/a-6419-0.html.

Dowel, T. (2016, August 31). Eminent Domain in Texas (Part 2) - Condemnation Proceedings Step by Step. Retrieved from https://agrilife.org/texasaglaw/2014/03/24/eminent-domain-in-texas-part-2-condemnation-proceedings-step-by-step/.

Enoch, C. (2019, March 26). High-speed rail has legal authority to keep moving forward. Retrieved from http://www.madisonvillemeteor.com/stories/high-speed-rail-has-legal-authority-to-keep-moving-forward,31199.

Ex Parte Davis. (n.d.). Retrieved from https://law.justia.com/cases/texas/court-of-criminal-appeals/1967/39935-3.html.

FindLaw's Court of Appeals of Texas case and opinions. (n.d.). Retrieved from https://caselaw.findlaw.com/tx-court-of-appeals/1123687.html.

FindLaws Court of Appeals of Texas case and opinions. (n.d.). Retrieved from https://caselaw.findlaw.com/tx-court-of-appeals/1696940.html.

Japan Bank for International Cooperation. (2016). *Jbic profile: role and function*. Tokyo.

Kelo v. New London, 545 U.S. 469 (2005). (n.d.). Retrieved from https://supreme.justia.com/cases/federal/us/545/469/.

Learn The Facts. (2019, September 25). Retrieved from https://www.texascentral.com/facts/.

Leopold, A. A. (2018). *Land Titles and Title Examination* (3rd ed., Vol. 5A). St. Paul, MN: West.

Lopez, R., Snelgrove, T., & Fitzsimons, B. (2014). Texas Land Trends. Retrieved from http://texaslandtrends.org/lt-2014-fact-sheet.pdf.

Martin, J. (2017, February 15). Texas high-speed rail company faces complicated battle over landowner access. Retrieved from https://www.bizjournals.com/houston/news/2017/02/15/texas-high-speed-rail-company-faces-complicated-ba.html.

Matthews, C. (2019, March 4). High-speed rail project to appeal railroad definition ruling. Retrieved from https://www.bizjournals.com/houston/news/2019/02/14/texas-central-plans-to-appeal-judges-recent.html.

Safety and Security: The Heart Of The Texas Train. (2019, January 14). Retrieved from https://www.texascentral.com/safety-security/.

Smith v. State. (n.d.). Retrieved from https://law.justia.com/cases/texas/court-of-criminal-appeals/1990/1432-88-4.html.

Staff, M. (2019, February 12). High-speed rail loses court case. Retrieved from http://www.madisonvillemeteor.com/stories/high-speed-rail-loses-second-court-case,31047.

Supreme Court of Texas. (n.d.). WALKER v. PACKER: 827 S.W.2d 833 (1992): w2d83311563. Retrieved from https://www.leagle.com/decision/19921660827sw2d83311563.

Tax Code. (n.d.). Retrieved from https://statutes.capitol.texas.gov/Docs/TX/htm/TX.311.htm.

Texas Department of Transportation v. Garcia. (n.d.). Retrieved from https://caselaw.findlaw.com/tx-court-of-appeals/1108989.html.

Texas Property Code. (n.d.). Retrieved from https://statutes.capitol.texas.gov/Docs/SDocs/PROPERTYCODE.pdf.
Texas Rice Land Partners Ltd. v. Denbury Green Pipeline-Texas LLC. (2012, March 6). Retrieved from https://www.law.com/texaslawyer/almID/1202544608410/?slreturn=20191112162600.
Texas Transportation Code. (n.d.). Retrieved from https://statutes.capitol.texas.gov/Docs/TN/htm/TN.112.htm.
The Project. (2019, November 21). Retrieved from https://www.texascentral.com/project/.
The Texas Bullet Train - Alignment Maps. (2019, January 14). Retrieved from http://devtxcentral.wpengine.com/alignment-maps/.
The Texas Constitution. (n.d.). Retrieved from https://statutes.capitol.texas.gov/Docs/CN/htm/CN.1.htm.
Thiel v. Harris Cty. Democratic Exec. Com. (n.d.). Retrieved from https://law.justia.com/cases/texas/supreme-court/1976/b-5863-0.html.

Journal of Business and Accounting
Vol 14, No 1; Fall 2021

THE RELATIONSHIP BETWEEN THE ETHICAL BEHAVIOR OF PEERS AND GRIT: EVIDENCE FROM UNIVERSITY BUSINESS CLASSES

Kevin Berry
Stacy Boyer-Davis
Northern Michigan University
Margaret Keiper
Jean Richey
University of Alaska Fairbanks

ABSTRACT

This study investigates whether Grit and its two components, the perseverance of effort and consistency of interest (passion), are related to the perceptions of the ethical behavior of peers. A sample of 232 undergraduate students from a university located in the northwest United States was used. Results indicate that when Grit is divided into its two components, each one is significantly related to the perceptions of the ethical behavior of peers. However, the perseverance of effort is negatively related, while the consistency of interest is positively related. Self-reported ethical behavior was positively associated with the perception of the ethical behavior of peers. None of the other dimensions of emotional intelligence were significant. Age and if the individual was a business major also had an impact on the perception of the ethical behavior of peers.

Key Words: Grit, effort, passion, ethical behavior, business, higher education

INTRODUCTION

The Association of Certified Fraud Examiners (ACFE) Report to the Nations 2018 Global Study on Occupation Fraud Abuse estimates that organizations lose 5% of their annual revenues due to fraud. According to the study, these frauds last an average of sixteen months, and nearly half (44%) are committed by employees who are not owners or in managerial roles. The study also found that in the United States (US), 58% of the frauds were committed by males and that, as the education level increases, the dollar size of the fraud also increases. Tips received through hotlines and other means are one of the main ways frauds are discovered. According to the study, approximately one-half of these tips come from current employees. Following this train of thought, the ability to predict which employees are more likely to commit theft or fraud, as well as which employees are more apt to offer information about fraudulent activities and uphold ethical standards in the first place, become of great interest.

As a result, the ability to screen potential employees and assign specific job positions utilizing ethically influencing characteristic measures is highly advantageous in the business setting, and research in this area has been encouraged in business for some time (Fritzsche, 1995). Over the years, several studies have identified many personal and societal/group characteristics and factors related to the ethical beliefs, intentions, decisions, and behaviors of employees. Among the more significant findings is the impact that the ethical behavior of peers has on the ethical behavior of people in the workplace (Ruiz-Palomino, Bañón-Gomis, & Linuesa-Langreo, 2019; Deshpande & Joseph, 2009; O'Fallon & Butterfield, 2012).

Recently, the concept of Grit has been suggested as a characteristic that can be used when considering the type of person to hire (Quinn, 2018; Lee & Duckworth, 2018). Grit is defined as the perseverance and passion for obtaining long-term goals. People who possess Grit are more likely to succeed in their long-term efforts (Duckworth, Peterson, Matthews, & Kelly, 2007). Eskreis-Winkler, Shulman, Beal, and Duckworth (2014) studied Grit and retention's relationship in four different contexts. They found that grittier soldiers were more likely to complete an Army Special Operations Forces (ARSOF) selection course, grittier sales employees were more likely to keep their jobs, grittier students were more likely to graduate from high-school, and grittier men were more likely to stay married. Duckworth, Quinn, and Seligman (2009) found that Grit was a significant predictor of teacher effectiveness. These findings and others have resulted in many practical articles that have been written about the use of Grit when considering the type of person to hire (Quinn, 2018; Lee & Duckworth, 2018). This, combined with information about the amount of fraud that is committed and stopped by employees, underlies the importance of studying the relationship between Grit and ethical behavior.

The purpose of this study was to determine if a relationship exists between ethical behavior and the trait of Grit. Specifically, the study investigates whether Grit is related to the perception of the ethical behavior of peers. Grit was considered as a lone construct and was also divided into its two components, the perseverance of effort and consistency of interest (passion). The analysis controlled for various demographic and emotional intelligence variables shown by prior research to be associated with the perception of the ethical behavior of peers.

LITERATURE REVIEW

Ethical Behavior of Peers

O'Fallen and Butterfield (2005) strongly suggested the need for additional research concerning peer influence on ethical behavior. Since that time, research results concerning the peer-ethical behavior connection have shown that these referent others have major influences regarding a person's ethical intentions. Decisions and actions that individual peers and peer groups with an inclination

towards unethical activities can influence the ethical behaviors of employees in the workplace (Ruiz-Palomino, Bañón-Gomis, & Linuesa-Langreo, 2019; Deshpande & Joseph, 2009; O'Fallon & Butterfield, 2012). Dimitriou and Ducette (2018) went as far as to say that "from a research standpoint...ethical behavior of peers is the most powerful and influential factor of ethical behavior across different industries, disciplines, and settings" (pg. 72).

Deshpande and Joseph (2009) analyzed survey responses of hospital nurses in the Midwest and Northwest USA. This study measured the impact of the ethical behavior of coworkers. The sample was part of a larger study consisting of 203 hospital employees that also included doctors, pharmacists, technicians, and office staff. Results indicated that the ethical behavior of coworkers had a significant impact on the nurses' ethical behavior. In addition, Deshpande (2009) also, using a portion of this larger survey, studied 180 of the subjects' responses in relation to the impact of ethical behavior of peers and found that ethical behavior of peers once again had a significant influence on an employee's ethical behavior. Fu and Deshpande (2012) studied factors impacting the ethical behavior of 208 employees at a Chinese steel company on mainland China. They found that the ethical behavior of peers was the most significant factor impacting the ethical behavior of these subjects. These researchers suggested that "if employees see that their coworkers...go unpunished if they perform deviant behavior or get rewarded for their unethical behavior, they are likely to also indulge in such behavior" (pg. 235).

Joseph, Berry, and Deshpande (2009) investigated factors that could influence the perception of ethical conduct of peers in 293 students from four universities in the Midwestern and Northwestern United States during late 2007 and early 2008. They found self-reported ethical behavior, others' emotional appraisal (one of the four dimensions of emotional intelligence from the Wong and Law Emotional Intelligence Scale), age, and majoring in business were significantly correlated with the ethical behavior of peers. Regression analysis revealed that the independent variables of ethical behavior of self and others' emotional appraisal significantly influenced ethical behavior of peers. However, age and majoring in business dropped out during the regression. All other independent variables (self-emotions appraisal, use of emotions, regulation of emotions, ethnicity, gender, grade point average, and over-claiming) were not found to influence the ethical behavior of peers to any degree.

Drawing from this same study, and looking more closely at business students specifically, Deshpande, Joseph, and Berry (2012) examined the ethical behavior of 193 participating business students. As with Joseph et al. (2009),

ethical behavior of self and others' emotional appraisal was found to be significantly correlated. Results from regression showed self-reported ethical behavior and two dimensions of emotional intelligence, self-emotional appraisal and others' emotional appraisal, significantly impacted the ethical behavior of peers. Again, as with Deshpande et al. (2009), grade point average, gender and over-claiming were not found to be significant. In addition, the authors found that the other independent variables of religiosity, whether the student had taken a non-business ethics course, graduate status, and the specific university the student attended, did not have a significant impact on the ethical behavior of peers.

Keiper, Berry, and Richey (2020) repeated the Joseph et al. (2009) study during the 2017-2018 school year (ten years later) utilizing a similar sample of students from the same Midwestern and Northwestern area of the United States. They found, just as both Joseph et al. (2009) and Deshpande et al. (2012) determined, that the ethical behavior of self significantly influenced the ethical behavior of peers. In addition, regulation of emotions, a facet of emotional intelligence, also significantly impacted the ethical behavior of peers. Keiper et al. (2020) also found that the impact on the perception of ethical behavior of peers depended on the year the data was collected. In the 2007-2008 collection, respondents perceived their peers to be more ethical than those students who completed the 2017-2018 survey.

All three research studies utilized college students from the same locations in the United States, the Midwestern and Northwestern areas specifically. All three found the ethical behavior of self and at least one of the four facets of emotional intelligence to significantly impact the ethical behavior of peers. In addition, several variables (self-reported ethical behavior, others' emotional appraisal, college major, specifically being a business student, and age) were found to be statistically correlated with the ethical behavior of peers in at least one of the studies. Per regression analysis, the following variables ultimately were not found to have any significant impact on the ethical behavior of peers in any of the completed studies that tested for them: age, gender, ethnicity, major, grade point average, religiosity, whether the student had taken a non-business ethics course, graduate status, specific university the student attended, use of emotions or over-claiming.

The Grit Construct

Duckworth et al. (2007) were the first to investigate Grit which entails working towards challenges and maintaining effort and interest over the years

despite failure, adversity, and plateaus in the process. To do so, they created a scale with 12 questions that were scored using a five-point Likert scale (Grit-O). They used the scale developed in six studies of diverse samples of people. Three of the studies were cross-sectional, and the other three were longitudinal. In the cross-sectional studies, they found that Grit helped to explain the variation in the educational attainment of adults over the age of 25 and that it was also positively related to the grade point average of Ivy League undergraduates. In the longitudinal studies, Grit predicted whether or not West Point Cadets would complete a rigorous summer training program and that finalists in the National Spelling Bee would be more likely to advance to further rounds.

In a later study, Duckworth and Quinn (2009) validated a more efficient measure of Grit (Grit-S) that used only eight questions and a five-point Likert scale. Again, they reported from six separate studies, two cross-sectional and four longitudinal. The two cross-sectional studies suggested that a two-factor model, passion (interest) and effort, was the best fit for the data. Results from the longitudinal studies indicated that Grit-S had a better fit than the twelve question Grit-O scale. Both Datu, Valdez, and King (2016) using a sample of university and high school students from the Phillipines, and Tyumeneva, Kardanova, and Kuzmina (2019), using a sample of Russian high school students, found evidence that Grit is comprised of two distinct constructs rather than one measure.

The short grit scale (Duckworth & Quinn, 2009) has been used broadly in social science research. Educational attainment was just one of the factors that have been researched to see if it has a relationship with Grit. Teacher effectiveness (Duckworth, Quinn, and Seligman, 2009), physician satisfaction (Reed, Schmitz, Baker, Nukui, & Epperly, 2012), and resident well-being (Salles, Cohen, & Mueller 2014) have been shown to be positively related to Grit. More recently, Isenberg, Brown, DeSantis, Veloski, and Hojat (2020) found that medical students with higher grit scores were likely to have high self-esteem and a high empathetic orientation in patient care. Three reviews of the literature on Grit have been performed to date. Datu, Yuen, and Chen (2017) provide a literature review on Grit in an academic setting. Crede, Tynan, and Harms (2017) provide a meta-analytic synthesis of Grit literature, while Stoffel and Cain (2018) provide a review of Grit literature within the health professions education.

The concept of Grit has been linked to hiring decision-making (Butz, Stratton, Trzebiatowski, & Hillary, 2019). Alston, Marsh, Castleberry, Kelley, and Boyce (2019) examined the importance of applicant characteristics versus achieved markers of academic success during hiring decisions of entry-level pharmacists. They surveyed 3,723 licensed pharmacists concerning how important they would consider/rank 48 applicant traits and how their presence or absence would impact a hiring decision. These 48 traits were divided into 24 academic ability success traits and 24 character traits, Grit being one of seven key life success predictors used to develop the latter. Grit-related traits included, for example, that the applying pharmacist "finishes whatever he or she starts," "tries very hard even after experiencing failure," and "gets over frustrations and set-backs quickly." Results showed that these and all of the other character traits ranked higher, and

nearly all were considered more important to have than the academic traits during a hiring consideration.

Employers also want to hire employees who handle stress well and manage exhaustion and the tendency for burnout; evidence suggests that Grit is a potential employee characteristic that could assist employers in hiring such individuals. Ceschi, Sartori, Dickert, and Constantini (2016) studied the health impairment process defined as "chronic job demands...depleting workers' stamina and resulting in burnout...causing further health problems" (pg. 1), counterproductive work behavior (CWB), and Grit in 208 employees in the private service sector. Results revealed that higher grit scores made an individual less vulnerable to the effects of stressful events and that for those with lower Grit scores, exhaustion had a stronger influence on CWB.

In addition, employers want to hire hard-working employees, resulting in good business or service outcomes. Again, there is support that employees with more Grit produce better end results. Duckworth et al. (2009) studied 390 novice teachers in the Teach for America program placed in under-resourced public schools nationwide. They specifically looked at the relationship between the Grit level of the teachers and the academic gains of their students over the course of one school year. Grit was found to have a significant positive influence on the student academic gains and that "the effect of Grit on [the academic gains due to the teachers'] performance was likely due to effort expanded during the school year" (pg. 545).

Although very little is written concerning the relationship between Grit and ethical behavior, research concerning the two is emerging. Amigud and Lancaster (2019) examined the reasons students give for seeking unacceptable levels of help completing their academic work. Although they did not formally administer a grit scale, they did find that a lack of perseverance was the top reason for outsourcing the work as a way to avoid any more of the "tedious, stressful, boring, or exhausting...suffering" (pg. 102) that the assignment was causing them. Rundle, Curtis, and Clare (2019) examined Grit as one of several psychological constructs as it relates to students' reasons for not engaging in contract cheating (paying a ghostwriter to complete an assignment). 604 Western Australian University students were asked a series of twenty-one questions. These questions loaded on five factors: 1) fear of detection and punishment; 2) self-efficacy and mistrust; 3) morality and norms; 4) lack of opportunity; 5) and motivation for learning. The students were studied using the Grit-S scale (Duckworth & Quinn, 2009) to measure the consistency of interest and perseverance of effort concerning their motivation to learn. Using each of the factors as a dependent variable, five regressions were run with the consistency of interest and perseverance of effort as two of the variables included in the models. They found that consistency of interest was positively related to the fear of detection and punishment, self-efficacy and mistrust, morality and norms, and lack of opportunity. Perseverance of effort was a positive and significant predictor of self-efficacy and mistrust, morality and norms, and motivation for learning.

HYPOTHESES

Nevins, Bearden, and Money (2007) explored the relationship between ethical values and an individual's long-term orientation. Their findings indicated a positive association between long-term perspectives on tradition and planning and ethical values. Similarly, individuals that possess more Grit have been shown to be more successful in achieving their long-term goals and overcoming difficulties in the course of achieving them. Therefore, it is hypothesized that individuals with more Grit are more likely to demonstrate a higher level of ethical behavior. This resulted in the first hypothesis stated in the alternative form.

H_{A1}: Perceived ethical behavior of peers is positively related to Grit.

Datu et al. (2016) and Tyumeneva et al. (2019) found evidence that Grit is comprised of two distinct constructs rather than one measure. The two constructs, the perseverance of effort and consistency of interest, resulted in the following hypotheses stated in the alternative.

H_{A2}: Perceived ethical behavior of peers is positively related to the consistency of interest.

H_{A3}: Perceived ethical behavior of peers is positively related to the perseverance of effort.

STUDY METHODOLOGY

Sample

A questionnaire was administered to undergraduate students at a university in the Northwestern United States. Survey administration occurred during the 2017-2018 academic year. The survey administration occurred mainly in business courses; however, several of these courses were highly enrolled by non-business majors as the courses fulfilled general education requirements at the given institution. Students were assured of anonymity and were given class time to complete the survey in-person. The survey took participants about 15 minutes to complete and was administered and collected by the course instructor. There was no incentive for participants to complete the survey. If a participant did not complete the entire survey or if questions were not answered, the survey was eliminated from the sample. In total, 261 surveys were collected, and 232 were deemed useable, giving the researchers a response rate of 89%.

Table 1
Frequency and Percentages of Dichotomous Categorical Variables (N = 232)

Variable	Frequency	Percentage
Gender (FEM) – Female	83	35.62%
Gender (FEM) – Male	150	64.38%
Business Major (BBA) – Majoring in Business	84	36.05%
Business Major (BBA) – Not Majoring in Business	149	63.95%
Engineering (ENG) – Majoring in Engineering	70	30.04%
Engineering (ENG) – Not Majoring in Engineering	163	69.96%
Upper Classman (JRSR) – Junior or Senior	112	48.07%
Upper Classman (JRSR) – Freshmen or Sophomore	121	51.93%

Table 1 lists the frequency and percentages of dichotomous categorical demographic variables. The sample consists of 83 females and 150 males. Seventy were engineering majors, 84 were business majors, and the remainder of the participants listed other majors. Finally, 112 were upperclassmen, juniors or seniors, and 121 were freshmen or sophomores.

VARIABLES AND MEASURES

Dependent Variable

The scale for the dependent variable, ethical behavior of peers (EBP), was used in several prior studies (for example, Joseph et al. 2009 and Keiper et al. 2020). This scale was originally developed based on the work of Jackson (2001) and Viswesvaran, Deshpande, and Joseph (2000). EBP was measured using 12 items. All items utilized within the EBS portions of the survey are presented in the Appendix. Items were rated on a four-point Likert scale (4 = very frequently, 1 = very infrequently). The Cronbach's alpha for EBP was $\alpha = .87$.

Test Variables

Duckworth et al. (2007) developed a twelve-item grit measure. Later the scale was reduced to eight items (Duckworth & Quinn 2009). This study uses the eight-item short Grit scale (Grit-s) to measure Grit and to test the first hypothesis. The scale includes four questions related to effort and four questions related to interest. All questions are measured using a five-point Likert scale. For those questions that relate to interest, the scale goes from one, being "very much like me," to five, being "not like me at all." Questions that relate to effort are measured on a scale where five is "very much like me," and one is "not like me at all." The scores from the eight questions are then averaged. The maximum score of five indicates someone is extremely gritty, while the low score of one indicates that the individual is not at all gritty. The Cronbach's alpha for EBP was $\alpha = .64$.

Control Variables

Personality, values, attitudes, teamwork, strengths, weaknesses, and many other factors have all been studied as factors contributing to ethical behavior (Lyons & Kuron 2014). This study controlled for ethical behavior of self, a variety of demographic factors, emotional intelligence, and overclaiming.

Similar to EBP, the ethical behavior of self (EBS) was also measured using 12 items, with items rated on a four-point Likert scale (4 = very frequently, 1 = very infrequently). The Cronbach's alpha for EBS was α = .76. Demographic factors controlled for include GPA, business major (BBA), engineering major (ENG), age, gender, and years of work experience.

The Wong and Law EI Scale (WLEIS) was utilized to measure emotional intelligence (Law, Wong & Song, 2004). The WLEIS is a self-reported scale, which consists of items used to measure the ability of a person to understand, regulate, and make use of her or his emotions. The WLEIS scale measures the latent construct of emotional intelligence and is comprised of four dimensions. The four dimensions are self-emotions appraisal (SEA), others emotions appraisal (OEA), use of emotions (UOE), and regulation of emotions (ROE). All items for the WLEIS scale are rated on a four-point Likert-type scale with 1 representing "strongly agree," 2 representing "agree," 3 representing "disagree," and 4 representing "strongly disagree.

In addition, an overclaiming scale was utilized in this study to control for social desirability bias in the survey. Overclaiming represents the participants' tendency to claim knowledge about things that do not exist, thus misrepresenting the knowledge of oneself. This study utilized the same technique as Joseph et al. (2009), where respondents were asked to rate their degree of familiarity with items that were nonexistent. The Cronbach's alpha for overclaiming was α = .81.

Regression Models

The research methodology consisted of estimating two regression models using a sample of students. Regression Model 1 was used to test the first hypothesis. It was estimated as follows:

$$EBS_i = B_0 + B_1EBP_i + B_2AGE_i + B_3YRSX_i + B_4FEM_i + B_5GPA_i + B_6JRSR_i + B_7BBA_i + B_8ENG_i + B_9SEA_i + B_{10}OEA_i + B_{11}UOE_i + B_{12}ROE_i + B_{13}OCLM_i + B_{14}GRIT_i + e_i$$

The dependent variable was the ethical behavior of peers (*EBP*). The test variable in Model 1, used to test the first hypothesis, was Grit (*GRIT*). Control variables for this regression included ethical behavior of self (*EBS*), age (*AGE*), years of experience (*YRSX*), gender (*FEM*), grade point average (*GPA*), business major (*BBA*), engineering major (ENG), self-emotional appraisal (SEA), regulation of emotion (ROE), use of emotion (UOE), others' emotional appraisal (OEA), and overclaiming (OCLM). Regression Model 2 was used to test the second and third hypotheses. It was estimated as follows:

$$EBS_i = B_0 + B_1EBP_i + B_2AGE_i + B_3YRSX_i + B_4FEM_i + B_5GPA_i + B_6JRSR_i + B_7BBA_i + B_8ENG_i + B_9SEA_i + B_{10}OEA_i + B_{11}UOE_i + B_{12}ROE_i + B_{13}OCLM_i + B_{14}GRITI_i + + B_{15}GRITE_i + e_i$$

The dependent variable was the ethical behavior of peers (*EBP*). The test variables in Model 2, used to test the second and third hypothesis, were GRITI (interest) and GRITE (effort). Again, the control variables for this regression included ethical behavior of self (*EBS*), age (*AGE*), years of experience (*YRSX*), gender (*FEM*), grade point average (*GPA*), business major (*BBA*), engineering major (ENG), self-emotional appraisal (SEA), regulation of emotion (ROE), use of emotion (UOE), others' emotional appraisal (OEA), and overclaiming (OCLM).

ANALYSIS AND RESULTS

Table 2 reports the means and standard deviations of the variables used in the study. The dependent variable, Ethical behavior of peers (EBP), was scored from 1 low ethical behavior to 4 high ethical behavior and had a mean of 2.69. As expected, individuals considered themselves more ethical than their peers as the variable ethical behavior of self (EBS) had a mean of 3.52. The average age of the sample was 23.21 with a standard deviation of 6.88 and the average years of work experience were 6.39 with a standard deviation of 6.19. These means appear to be higher than for the typical undergraduate student and are reflective of a sample taken from a university that serves a high percentage of non-traditional students. GRIT was measured on a scale from 1 to 5 and had an average score of 2.58. Separating Grit into its two components, interest and effort, yielded an average of 3.00 for GRITI and 2.16 for GRITE.

Table 2
Descriptive Statistics (N = 232)

Variable	Mean	Std. Deviation
Ethical Behavior of Peers (EBP)	2.69	.60
Ethical Behavior of Self (EBS)	3.52	.37
Age (AGE)	23.21	6.88
Years of Experience (YRSX)	6.39	6.19
Grape Point Average (GPA)	3.23	.51
Overclaiming (OCLM)	2.93	.17
Self-Emotional Appraisal (SEA)	1.89	.63
Others' Emotional Appraisal (OEA)	2.09	.59
Use of Emotions (UOE)	1.91	.64
Regulation of Emotions (ROE)	1.93	.61
GRIT – Full Measure (GRIT)	3.45	.62
GRIT – Passion (GRITI)	3.91	.72
GRIT – Perseverance (GRITE)	3	.81

Correlations

Table 3 indicates the correlations among variables for Model 1. Years of experience (YRSX) and age (AGE) were highly correlated with each other at .83. Similarly, AGE and YRSX are correlated with upperclassmen (JRSR). These results were not surprising as older students would be expected to have more years of work experience as well as be further along in their studies. Identifying as female gender (FEM) and identifying as an engineering (ENG) major was moderately negatively correlated, which also was not surprising as engineering is

historically a male-dominated field. The emotional intelligence variables for others' emotional appraisal (OEA), regulation of emotions (ROE), and use of emotions (UOE) were all correlated with self-emotional appraisal (SEA). Grit was also highly negatively correlated with the use of emotion (UOE). Lastly, Ethical behavior of self (EBS) and overclaiming (OCLM) were correlated, which is explained by a common limitation with any self-report measure.

Table 3
Model 1 Correlations Among Variables

Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. EBS	1.00													
2. AGE	.07	1.00												
3. YRSX	.12	.83	1.00											
4. FEM = 1	.14	.07	.05	1.00										
5. GPA	.05	-.04	.03	.06	1.00									
6. JRSR	.10	.35	.30	.11	-.02	1.00	.							
7. BBA = 1	.08	.06	.05	.26	-.05	.03	1.00							
8. ENG = 1	-.08	-.19	-.20	-.29	-.03	-.10	-.49	1.00						
9. OCLM	.38	.11	.11	.06	-.03	.05	.10	-.16	1.00					
10. SEA	.01	-.12	-.16	.10	-.12	.05	.04	-.05	.03	1.00				
11. OEA	-.10	-.13	-.11	-.22	-.13	-.01	-.04	.17	.00	.37	1.00			
12. UOE	-.07	-.05	-.06	-.08	-.16	-.02	-.02	.08	.08	.42	.26	1.00		
13. ROE	-.03	.05	.03	.20	-.11	.01	.10	-.08	.03	.47	.24	.21	1.00	
14. GRIT	.13	.05	.09	.10	.11	-.05	-.01	-.13	-.07	-.22	-.22	-.47	-.09	1.00

For Model 2, the correlations among variables are shown in Table 4. Similar to Model 1, YRSX and AGE were highly correlated, and AGE and YRSX were again correlated with JRSR. The same correlation between being an engineering major and female also existed. The same correlations between the emotional intelligence variable existed as it did in Model 1. Consistency of interest (GRITI) and perseverance of effort (GRITE) were negatively correlated with ROE at -.38 and -.39, respectively. GRITI and GRITE were positively correlated at .34.

Table 4
Model 2 Correlations among Variables

Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. EBS	1.0														
2. AGE	.07	1.0													
3. YRSX	.12	.83	1.0												
4. FEM = 1	.14	.07	.05	1.0											
5. GPA	.05	-.04	.03	.06	1.0										
6. JRSR	.10	.35	.30	.11	-.02	1.0									
7. BBA = 1	.08	.06	.05	.26	-.05	.03	1.0								
8. ENG = 1	-.08	-.19	-.20	-.29	-.03	-.10	-.49	1.0							
9. OCLM	.38	.11	.11	.06	-.03	.05	.10	-.16	1.0						
10. SEA	.01	-.12	-.16	.10	-.12	.05	.04	-.05	.03	1.0					
11. OEA	-.10	-.13	-.11	-.22	-.13	-.01	-.04	.17	.00	.37	1.0				
12. UOE	-.07	-.05	-.06	-.08	-.16	-.02	-.02	.08	.08	.42	.26	1.0			
13. ROE	-.03	.05	.03	.20	-.11	.01	.10	-.08	.03	.47	.24	.21	1.0		
14. GRITE	.11	.03	.02	.09	.03	.00	.03	-.13	-.02	-.15	-.15	-.38	-.04	1.0	
15. GRITI	.10	.06	.12	.07	.14	-.08	-.04	-.09	-.08	-.21	-.21	-.39	-.11	.34	1.0

Hypothesis Testing Results

Model 1 was used to test the first hypothesis. Using Model 1, a multiple linear regression was run to predict the ethical behavior of peers on 14 predictor variables, as shown in Table 5. A significant regression equation was found R^2 = .25, $F(14, 217) = 5.044, p < .01$, as 14 predictors explained 25% of the variance. The analysis of Model 1 shows that the full measure of Grit (GRIT) did not significantly predict the perceived ethical behavior of peers, and therefore, there was no support for the first hypothesis. The analysis of Model 1 showed that the control variables of AGE (t = 1.78, p < .10) and BBA (t = 1.80, p < .10) significantly predicted perceived ethical behavior of peers. EBS, ethical behavior of self also significantly predicted the perceived ethical behavior of peers (t = 7.05, p < .01).

Table 5
Regression Analyses for Ethical Behavior of Peers (EBS)

	Model 1		*Model 2*	
Variable	*β*	*t*	β	*T*
Ethical Behavior of Self (EBS)	.47	7.05***	.47	7.18**
Age (AGE)	.20	1.78*	.21	1.92*
Years of Experience (YRSX)	-.07	-.60	-.10	-.88
Gender (FEM)	-.08	-1.21	-.08	-1.24
Grade Point Average (GPA)	-.02	-.264	-.03	-.48
Upper Classman (JRSR)	-.04	-.70	-.03	-.48
Business Major (BBA)	.13	1.80*	.13	1.90*
Engineering Major (ENG)	.12	1.60	.11	1.54
Overclaiming (OCLM)	-.04	-.69	-.04	-.59
Self-Emotional Appraisal (SEA)	.03	.45	.03	.43
Others' Emotional Appraisal (OEA)	-.06	-.85	-.05	-.78
Use of Emotions (UOE)	.01	.08	.00	.02
Regulation of Emotions (ROE)	-.05	-.77	-.05	-.68
GRIT – Full Measure	.04	.51		
GRIT – Passion (GRITI)			-.12	-1.85*
GRIT – Perseverance (GRITE)			.16	2.38**
R^2	.25		.27	

Note. * $p < .10$, ** $p < .05$, *** $p < .01$.

To test the second and third hypotheses, regression Model 2 was calculated to predict the ethical behavior of peers using 15 test and control variables, as shown in Table 5. A significant regression equation was found, R^2 = .27, $F(15, 216) = 5.328, p < .01$, as 15 predictors explained 27% of the variance. The analysis of Model 2 showed that consistency of interest or passion (GRITI) significantly predicted the perceived ethical behavior of peers (t = 2.38, p < .05), and thus there is support for the second hypothesis. The analysis of Model 2 shows that perseverance of effort (GRITI) was negative and significantly predicted the perceived ethical behavior of peers (t = -.121, p < .1). As a result of the negative coefficient, there is no support for the third hypothesis. Similar to the first model, Model 2 also shows that AGE and BBA significantly predicted the perceived ethical behavior of peers at the p < .1 level. Again, EBS also predicted the perceived ethical behavior of peers at p < .01.

LIMITATIONS

Like any study, this study has limitations. First, the study used a convenience sample. This sample may not be representative of students across the nation. Second, although the study controlled for many demographic

variables that were based on previous research, the study did not control for all possible factors. Many situational and personality factors could also have affected the results of the study.

IMPLICATIONS

This study has both implications for future research and practical implications. Future research needs to be conducted on different age groups to see if age and the Grit relationship to ethical behavior exists. Duckworth and Quin (2009) also found that the older groups had higher levels of Grit. Given that hiring employees is often done by non-peer individuals, it would be important to investigate the relationship between the components of Grit and other variables and the perception of the ethical behavior of groups that would not be considered peers. Finally, the results of this study and those of Rundle et al. (2019) suggest that further research needs to be done to establish if there is a direct relationship between Grit and ethical decision making or if there is an intermediate step such as a relationship between Grit and the opportunity to commit unethical behavior that is driving the results.

The result from this study also has practical implications. The result implies that hiring individuals that demonstrate passion or consistency of interest could help to change the culture of an organization to be one that is more ethical. However, the results also indicate that individuals with high perseverance of effort may view their peers as having poor ethical behavior. This could have a negative effect on the culture of an organization, and therefore appropriate training and discussion need to take place to mitigate any negative behavior that may result because of this relationship. This could also impact the hiring process by prompting specific questions about the consistency of interest (passion) during job interviews and when contacting candidates' references.

CONCLUSION

The purpose of this study was to examine the relationship between ethical behavior and Grit. Using the ethical behavior of peers as the dependent variable, three hypotheses were tested. There was no support for the first hypothesis that Grit, measured by using the eight-question short scale (Grit-s), was positively related to the ethical behavior of peers. The second and third hypotheses considered the two dimensions of Grit as separate constructs. The second hypothesis looked at the relationship between consistency of interest (passion) and the ethical behavior of peers. The third hypothesis examined the relationship between the perseverance of effort and the ethical behavior of peers. The results of the study found support for the second hypothesis, which indicates that the higher an individual's consistency of interest (GRITI), the higher they view the ethical behavior of their peers. Although there was no support for the third hypothesis, that perseverance of effort (GRITE) is positively related to the ethical behavior of peers, the test variable was marginally significant (p-value = .066) but negative.

Consistency of interest being significant and positively related to ethical behavior is consistent with the results of Rundle et al. (2019). However, this study examines the concept of Grit and ethics versus studying the relationship between a reason for not committing the ethical violation of contract cheating. Perseverance of effort (GRITE) was found to be negatively correlated with the perceived ethical behavior of peers, whereas Rundle et al. (2019) found that it was positively correlated with several of the factors for why students would not commit contract cheating. This is interesting as it indicates that the higher an individual's perseverance of effort, the lower they consider the ethical behavior of their peers.

The control variable for age was also significant, indicating that older students perceived their peers as more ethical. Based on our sample of respondents, we find that age does significantly impact ethical behavior, measured here by the ethical behavior of peers; this reveals more evidence that as age increases, so does positive ethical behavior. These findings contradict those studies that have detected either a negative impact on ethical behavior (as age goes up, positive ethical behavior goes down) or no age differences regarding ethical judgment (Sankaran & Bui, 2003; Fu, 2014; However, Byrne & Trushell, 2013; Deshpande, Joseph, & Berry, 2012; Andreoli & Lefkowitz, 2009).

However, our findings are consistent with other studies that have detected age differences. Similar to our findings, this research has found that older students are more ethical than younger ones. Specifically, these studies report that older students intend to believe they would and act more ethically than their younger counterparts (Klein, Levenburg, McKendall & Mothersell, 2007; Borkowski & Ugras, 1998; Ruegger & King, 1992; Comer & Vega, 2008; Kisamore, Stone, & Jawahar, 2007). Evidence suggests that students 40 years and older are more ethical than their younger peers (Ruegger & King, 1992).

Additional research studies also found that older employees tended to be more ethical (Kim & Chun, 2003; Hunt & Jennings, 1997). Peterson, Rhoads, and Vaught (2001) and Kelley, Ferrell, and Skinner (1990) found that professionals above specific ages rated themselves more ethical than younger employees (above age 30) and reported that their beliefs were less influenced by external ethical factors (above age 50) respectively.

The variable for those majoring in business (BBA) was positive and marginally significant, indicating that business majors viewed their peers as more ethical, which is in contrast to other studies that investigated unethical behavior and college major. Specifically, results from other studies report that business students have lower ethical standards, more unethical behavior, including cheating, and are laxer concerning their point of view of what they constitute as cheating (McCabe & Treviño, 1995; Klein et al., 2007; Harris, 1989; McCabe, Butterfield, & Trevino, 2006; Gallant & Binkin, 2015; Carauna & Ewing, 2000).

REFERENCES

Alston, G. L., Marsh, W., Castleberry, A.N., Kelley, K.A., & Boyce, E.G. (2019). Pharmacists' opinions of the value of specific applicant attributes in hiring decisions for entry-level pharmacists. *Research in Social and Administrative Pharmacy, 15,* 536-545.

Amigud A., & Lancaster T. (2019). 246 reasons to cheat: An analysis of students' reasons for seeking to outsource academic work. *Computers and Education, 134,* 98-107.

Andreoli, N., & Lefkowitz, J. (2009). Individual and organizational antecedents of misconduct in organizations. *Journal of Business Ethics, 85*(3), 309-332.

Association of Certified Fraud Examiners. (2018). Report to the Nations: 2018 Global study on occupational fraud and abuse.

Borkowski, S.C., & Ugras, Y.J. (1998). Business students and ethics: A meta-analysis. *Journal of Business Ethics, 17*(11)**,** 1117–1127.

Butz, N. T., Stratton, R., Trzebiatowski, M. E., & Hillary, T. P. (2019). Inside the hiring process: How managers assess employability based on grit, the big five, and other factors. *International Journal of Business Environment, 10*(4), 306-328.

Byrne, K., & Trushell, J. (2013). Education undergraduates and ICT-enhanced academic dishonesty: A moral panic? *British Journal of Educational Technology, 44(*1), 6-19.

Carauna, A., & Ewing, M. T. (2000). The effect of anomie on academic dishonesty in university students. *The Journal of Educational Management, 14*(1): 23-29.

Ceschi, A., Sargon, R., Dickert, S., & Constantini, A. (2016). Grit or honesty-humility? New insights into the moderating role of personality between the health impairment process and counterproductive work behavior. *Frontiers in Psychology, 7* (1799).

Comer, D. R., & Vega, G. (2008). Using the PET assessment instrument to help students identify factors that could impede moral behavior. *Journal of Business Ethics, 77*(2), 129-145.

Crede, M., Tyann, M. C., & Harms, P. D. (2017). Much ado about grit: A meta-analytic synthesis of the grit literature. *Journal of Personality and Social Psychology, 113*(3), 492-511.

Datu, J. A. D., Valdez, J. P. M., & King, R. B. (2016). Perseverance counts but consistency does not! Validating the short grit scale in a collectivist setting. *Current Psychology, 35*, 121-130.

Datu, J. A. D., Yuen, M., & Chen, G. (2017). Grit and determination: A review of literature with implications for theory and research. *Journal of Psychologists and Counsellors in Schools, 27*(2), 168-176.

Deshpande, S. P., (2009). A study of the ethical decision making by physicians and nurses in hospitals. Journal of Business Ethics, 90(3), 387-397.

Deshpande, S. P., & Joseph, J. (2009). Impact of emotional intelligence, ethical climate, and behavior of peers' ethical behavior. Journal of Business Ethics, 85(3), 403-410.

Deshpande, S. P., Joseph, J., & Berry, K. (2012). Ethical misconduct of business students: Some new evidence. *American Journal of Business Education, 5*(6), 719-725.

Dimitriou, C. K., & Ducette, J. (2018). An analysis of the key determinants of hotel employees' ethical behavior. Journal of Hospitality and Tourism Management, 34, 66-74.

Duckworth, A. L., Peterson, C., Matthews, M. D., & Kelly, D. R. (2007). Grit: Perseverance and passion for long-term goals. Journal of Personality and Social Psychology, 9, 1087-1101.

Duckworth, A. L., & Quinn, P. D. (2009). Development and validation of the Short Grit Scale (GRIT-S). Journal of Personality Assessment, 91(2), 166-174.

Duckworth, A. L., Quinn, P. D., & Seligman, M. E. P. (2009). Positive predictors of teacher effectiveness. The Journal of Positive Psychology, 4(6), 540-547.

Eskreis-Winkler, L., Shulmn, E.P., Beal, S.B., & Duckworth, A.L. (2014). The grit effect: predicting retention in the military, the workplace, school and marriage. Frontiers in Psychology, 5(36), 1-12.

Falk, A., & Ichino, A. (2006). Clean evidence on peer effects. Journal of Labor Economics, 24(1), 39-57.

Fritzsche, D. J. (1995). Personal values: Potential keys to ethical decision making. Journal of Business Ethics, 14(11), 909-922.

Fu, W. (2014). The impact of emotional intelligence, organizational commitment, and job satisfaction on ethical behavior of Chinese employees. *Journal of Business Ethics, 122*(1), 137-144.

Fu, W., & Deshpande, S. P., (2012). Factors impacting ethical behavior in a Chinese state-owned steel company. *Journal of Business Ethics, 105*(2), 321-237.

Gallant, T. B., & Binkin, N. (2015). Students at risk for being reported for cheating. *Journal of Academic Ethics, 13*, 217-228.

Harris, J. R. (1989). Ethical values and decision processes of male and female business students. *Journal of Education for Business, 64*(5), 234-238.

Hunt, T. G., & Jennings, D. F. (1997). Ethics and performance: A simulation analysis of team decision making. *Journal of Business Ethics, 16*(2), 195-203.

Isenberg, G., Brown, A. M., DeSantis, J., Veloski, J., & Hojat, M., (2020). The relationship between grit and selected personality measures in medical students. International Journal of Medical Education, 11, 25-30.

Jackson, T. (2001). Cultural values and management ethics: A 10-nation study. *Human Relations, 54*, 1267-1302

Joseph, J., Berry, K., & Despande, S. P. (2009). Impact of emotional intelligence and other factors on perception of ethical behavior of peers. Journal of Business Ethics. 89(4), 539-546.

Keiper, M., Berry, K. and Richey, J. (2020). Factors influencing perception of ethical behaviour of peers: Time, emotional intelligence, and ethical behaviour of self. *e-Journal of Business Education & Scholarship of Teaching*, *14*(1), 189-203.

Kelley, S. W., Ferrell, O. C., & Skinner, S. J. (1990). Ethical behavior among marketing researchers: An assessment of selected demographic characteristics. Journal of Business Ethics 9(8), 681–688.

Kim, S. Y., & Chun, S. Y. (2003). A study of marketing ethics in Korea: What do Koreans care about? *International Journal of Management, 20*(3), 377-383.

Kisamore, J. L., Stone, T. H., & Jawahar, I. M. (2007). Academic integrity: The relationship between individual and situational factors on misconduct contemplations. *Journal of Business Ethics, 75*(4), 381–394.

Klein, H. A., Levenburg, N. M., McKendall, M., & Mothersell, W. (2007). Cheating during the college years: How do business school students compare? Journal of Business Ethics, 72(2), 197–206.

Law, K., Wong, C., & Song L. (2004). The construct and criterion validity of emotional intelligence and its potential utility for management studies. *The Journal of Applied Psychology*, *89*(3), 483–496.

Lee, T. H., & Duckworth, A. L. (2018). Organizational grit. *Harvard Business Review, 96*(5), 98-105.

Lyons, S., & Kuron, L. (2014). Generational differences in the workplace: A review of the evidence and directions for future research. Journal of Organizational Behavior, 35(S1), S139-S157.

Ludeke, S. G., & Makransky, G. (2016). Does the over-claiming questionnaire measure overclaiming? Absent convergent validity in a large community sample. *Psychological Assessment, 28*(6), 765-774.

McCabe, D. L., Butterfield, K. D., & Trevino, L. K. (2006). Academic dishonesty in graduate business programs: Prevalence, causes, and proposed action. *Academy of Management Learning & Education, 5*(3), 294-305.

McCabe, D. L., & Treviño, L. K. (1995). Cheating among business students: A challenge for business leaders and educators. Journal of Management Education, 19(2), 205-218.

Nevins, J. L., Bearden, W. O., & Money, B. (2007). Ethical values and long-term orientation. Journal of Business Ethics, 71(3), 261-274.

O'Fallon, M. J., & Butterfield, K. D. (2012). The influence of unethical peer behavior on observers' unethical behavior: A social cognitive perspective. The Journal of Business Ethics, 109(2), 117-131.

Peterson, D., Rhoads, A., & Vaught, B. C. (2001). Ethical beliefs of business professionals: A study of gender, age and external factors. *Journal of Business Ethics*, *31*(3), 225-232.

Quinn, C. (2018). Hiring for attitude: How to identify motivation & grit during interviews. The HR Specialist, September, 4.

Reed, A. J., Schmitz, D., Baker, E., Nukui, A., & Epperly, T. (2012). Association of 'grit' and satisfaction in rural and nonrural doctors. *Journal of the American Board of Family Medicine*, *25*, 832–839.

Ruegger, D., & King, E. W. (1992). A study of the effect of age and gender upon student business ethics. *Journal of Business Ethics, 11*(3), 179-186.

Ruiz-Palomino, P., Bañón-Gomis, A., & Linuesa-Langreo, J. (2019). Impacts of peers' unethical behavior on employees' ethical intention: Moderated mediation by Machiavellian orientation. Business Ethics: A European Review, 28, 185-205.

Rundle, K., Curtis G. J., & Clare, J. (2019). Why students do not engage in contract cheating. Frontiers in Psychology, 10(2229).

Sankaran, S., & Bui, T. (2003). Relationship between student characteristics and ethics: Implications for educators. *Journal of Instructional Psychology, 30*(3), 240-253.

Salles, A., Cohen, G.L., & Mueller, C.M. (2014). The relationship between grit and resident well-being. *The American Journal of Surgery*, *207*, 251–254.

Stoffel, J. M., & Cain, J. (2018). Review of grit and resilience literature within health professions education. American Journal of Pharmaceutical Education, 82(2), 124-134.

Tyumeneva, Y., Kardanova, E., & Kuzmina, J. (2019). Grit: Two related but independent constructs instead of one. Evidence from item response theory. *European Journal of Psychological Assessment, 35*(*4),* 469–478.

Viswesvaran, C., Deshpande, S. P., & Joseph, J. (2000). Are ethical perceptions of various practices affected by workplace dependencies? *Journal of Applied Social Psychology, 30*(10), 2050-2057.

Westerman, J.W., Beekun, R.I., Stephan, Y., & Yamamura, J. (2007). Peers versus national culture: An analysis of antecedents to ethical

decisionmaking. Journal of Business Ethics, 75(3), 239-252.

APPENDIX

Instruments used to measure various constructs

Ethical behavior of peers

a) Students make personal calls at work.
b) Students surf the web at work.
c) Students take office supplies home.
d) Students share music on the internet.
e) Students download term papers off the internet.
f) Students give friends an extra discount at a store or free food at a cafe or restaurant.
g) Students sometimes help themselves to food if working at a fast food joint.
h) Students do homework for friends.
i) Students have used fake ID to purchase alcohol.
j) Students have used fake ID to get into a bar.
k) Students have cheated on an exam.
l) In order to get ahead in life, students believe that one has to compromise on ethical standards.

Ethical behavior of self

a) I'd make personal calls at work.
b) I'd surf the web at work.
c) I'd take office supplies home.
d) I'd share music on the internet.
e) I download term papers off the internet.
f) I'd give a friend an extra discount at a store or free food at a cafe or restaurant.
g) I'd sometimes help myself to food if I worked at a fast food joint.
h) I'd do homework for my close friends.
i) I've used fake ID to purchase alcohol.
j) I've used fake ID to get into a bar.
k) I've cheated on an exam.
l) In order to get ahead in your future career you will have to compromise your ethical standards.

Overclaiming scales

a) How familiar are you with each of the following movies?
    a. Turned to Gold Katherine's Mistake
    b. 544 Jacob Joseph et al.
b) How familiar are you with each of the following products?
    a. Microsoft Statistical Assistant
    b. New Life Spices

c) How familiar are you with the following albums?
    a. Cosmic Being
    b. Offender After Dark
d) How familiar are you with each of the following TV programs?
    a. The Adventure of Johnnie
    b. Chicago Heat
e) How familiar are you with each of the following designer labels?
    a. Ocean City
    b. Jones, L.A

Journal of Business and Accounting
Vol 14, No 1; Fall 2021

RANSOMWARE: HEALTHCARE INDUSTRY AT RISK

Susan Kiser
Balasundram Maniam
Sam Houston State University

Abstract
Malicious software, or malware as it is commonly known, has been around for hackers to employ for many years. Through an extension of malware, cybercriminals have evolved the technology and unleashed ransomware attacks. These vicious attacks hold businesses hostage as they lock down their computer systems and confiscate their data. Hackers then demand a ransom payment in exchange for an electronic key to unlock their systems and purchase their own data back. While these ransomware attacks are prevalent across the globe today, they are even more widespread throughout the healthcare industry. The objective of this paper is to highlight the risk the healthcare industry is under due to the increased number and evolving technology of ransomware attacks. This is accomplished through evaluating several areas. First, there are reasons presented explaining why the healthcare industry is specifically targeted. Second, there is discussion regarding the dilemmas healthcare organizations face during and after a cyber-attack. Third, there are explanations of the financial losses and medical care interruptions that occur when a health provider is under attack. Finally, there is discussion about specific ways healthcare organizations can minimize the risk of ransomware attacks.

Keywords*:* ransomware, malware, cyber-attack, healthcare industry, ransom payment, hacker, cybercriminal, cyber insurance

Introduction

Ransomware, a type of malicious software used by cybercriminals to impede access to computer systems until payment is made, is a growing industry in the United States and beyond. Although this type of destructive scheme has been around for many years, the impact shifted significantly in 2017 as sophisticated computer hacking evolved from targeting individuals to attacking large-scale businesses and organizations. Currently, this is a flourishing billion-dollar industry which threatens to disrupt and potentially destroy the enterprises it holds ransom (Zimba & Chishimba, 2019). As the drivers of this industry seek to streamline operations and increase profits,

they strategically choose their victims. Unfortunately, some of the most vulnerable organizations are located in the healthcare industry.

As technology has increased, the healthcare industry has embraced it and therefore become more connected to internet and cloud-based infrastructures. While this has been immensely helpful in regard to the level of medical care and information readily available, it has also proved to be the object of many cyber-attacks. In this paper, arguments will be presented to show that the healthcare industry is at increased risk due to ransomware attacks. This paper will proceed with a literature review, followed by an introduction to ransomware risks associated with the healthcare industry. This will then lead to three areas of exploration: reasons the healthcare industry is at risk, dilemmas created by the ransomware attacks, and financial and healthcare implications of the attacks. Following this will be an analysis of findings and the conclusion.

Literature Review

Several studies have been conducted on the subject of ransomware in the medical field. These include identifying and preventing malware, vulnerability with remote medical devices, and technical and economic impacts of ransomware attacks.

"Ransomware Trends 2021" published by the Department of Health and Human Services found that during the first five months of the year, there were 82 different ransomware attacks on the healthcare industry and 59% of them impacted U.S. healthcare organizations. In addition, the research showed that 72% of incidents resulted with victim data leaked. The average ransomware payment was $131,000. One of the dangers with malicious software, also known as malware, is that it can go undetected while executing its malicious code, causing damage before it is discovered. In a study by Or-Meir, Nissim, Elovici & Rokach (2019), existing techniques used to analyze malware were reviewed. This study showed that notable progress had been made since the last study on this subject was conducted in 2012. Specifically, the dynamic malware analysis showed that improvements had been made in the areas of performance, detection rates and increased resilience. A few years later, Pagán & Elleithy (2021) studied a preventative approach and found that a multi-layered strategy was best to prevent ransomware and minimize impact. In stretching beyond the Information Technology (IT) systems usually targeted, Nichol (2021) cited recent ransomware attacks and studied the possibility of malware reaching to the Operational Technology (OT) side of the systems. This side of the system includes devices, communication procedures, operating systems and software which is separate from the IT systems. Nichol (2021) concluded

that an OT attack could be politically motivated and lead to equipment failure, environmental repercussions and human injury.

As technology has developed, it has paved the way for many advances in the medical field, including portable machines. The Internet of Medical Things (IoMT) refers to mobile healthcare devices that enable remote monitoring. Items such as breathing sensors, motion sensors and blood pressure sensors are examples of IoMT's (Kumar, Gupta & Tripathi, 2020). While this technology has enabled many advancements in the medical field, it has also broadened the potential area of cyber-attack. In 2019, Abraham, Chatterjee & Sims published a study which looked into the cybersecurity challenges in the healthcare industry, such as the increase in potential attack surface with IoMT's. At the end of the study, they concluded that a comprehensive cybersecurity plan should include preventive, detective and recovery steps. Kumar, Gupta & Tripathi (2020) further studied the vulnerability that IoMT systems and devices present and proposed a fog-cloud architecture to detect any cyber-attacks. The experimental study showed that the software had a detection rate of 99.98% and accuracy rate of 96.35%.

Aside from preventing ransomware attacks in the healthcare industry, Zimba & Chishimba (2019) focused on the technical and economic aspects of an attack. This study noted that the primary targets include the healthcare industry and spam emails are the main pathway that ransomware enters the computer system. In addition, the study concluded that economic impacts include payment to criminals as well as recovery efforts and loss of production during the downtime.

Ransomware Risks Related to the Healthcare Industry

According to Abraham, Chatterjee & Sims (2019), cyberattacks on healthcare organizations have increased by 125% since 2014. The objective of this paper is to discuss the risks associated with the healthcare industry due to the ransomware attacks. This will be done by evaluating several areas. First, propositions will be made to show the reasons the healthcare industry is specifically targeted. These reasons vary from elements that could be changed to ones that are an integral part of this specific industry. Second, this paper will explore the dilemma health centers face when they are targeted by ransomware. Choosing whether to make the ransom payment is a weighty decision that affects much more than just their bank account. Third, the study will address the risks associated with these attacks, including financial and patient care implications. The nature of these risks can be severe not only for survival of the individual healthcare organizations but also greatly impact the health and well-being of individuals who seek treatment from these organizations. Finally, this

analysis will look at the potential solutions to minimize the risks associated with this evolving concern in the healthcare industry.

Reasons the Healthcare Industry is at Risk

Fundamentally, there are several reasons the healthcare industry is under more risk for ransomware attacks than other industries. Among these are the facts that they house sensitive information in their system, there is a higher probability of payment, there is an increased surface area of potential attack with IoMT's, there is insufficient training of employees and there is generally insufficient IT/cybersecurity protection.

While the healthcare industry has always kept medical records and patient data, technology advancements have increased the potential access to this information. According to the AMA Journal of Ethics, when the Health Information Technology for Economic and Clinical Health Act (HITECH) was signed into law in 2009, it brought "the most sweeping health care reform measures since Medicare" (Burde, 2011; Harkins & Freed, 2018). These changes included moving paper health records online in order to create electronic health records (EHRs). While use of this technology has been extremely helpful in connecting medical personnel with a patient's health information, it has also made the sensitive data extremely vulnerable as it can be accessed from anywhere in the world. In the years since EHRs were created and uploaded to hospital and healthcare networks, cases of cyberattacks on the medical industry have increased significantly (Harkins & Freed, 2018).

Once criminals have retrieved health records, they have a few different options for profiting from it. First, they can demand a ransom payment in exchange for returning it. Second, they can commit identity theft in order to obtain free medical procedures or prescriptions. Third, they can resell the valuable information on the black market (Harkins & Freed, 2018). While it is common knowledge that organizations in the medical industry house personal health information (PHI), the value of this information on the black market is widely underrated. According to Harkins & Freed (2018), PHI data is more profitable for criminals than personal information retrieved from the financial industry. In fact, the FBI Cyber Division published a report showing that while cyber criminals can expect to receive $1 per stolen social security number or credit card number, they can demand $50 for a partial health record ("Healthcare Systems", 2014; Harkins & Freed, 2018). This valuable PHI is one of main reasons the healthcare industry is under risk for ransomware attacks. Recognizing the urgent issue at hand, the U.S. Department of Health & Human Services recently created the Health Sector Cybersecurity Coordination Center (HC3) to help protect important medical information and make sure that

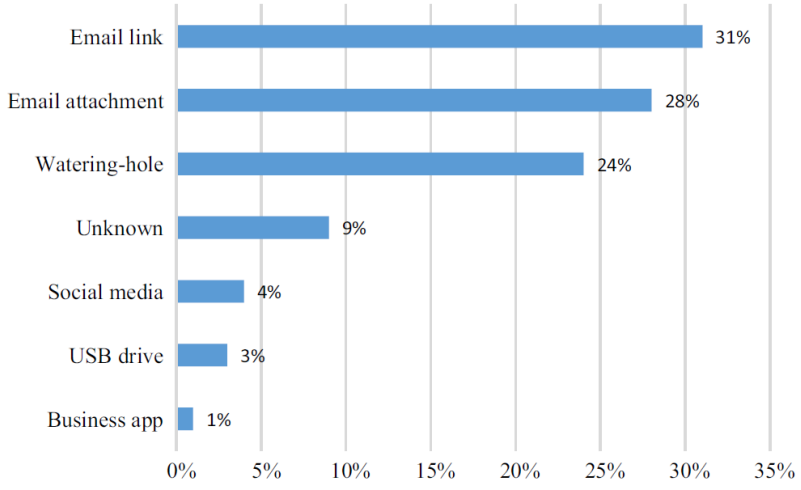
cybersecurity knowledge is coordinated across the Health and Public Health Sector (HPH)" (www.hhs.gov).

Another key motivation for cybercriminals to strike at the healthcare industry is the high probability of ransomware payment. As previously discussed, healthcare organizations house sensitive patient information, which they are morally and legally obligated to protect. If these requirements are not met, health care providers are in danger of facing remediation costs, legal fines, customer notification, damage to their brand and loss of business, all which are very costly (Chung, 2020). In fact, Chung's (2020) research highlighted a statistic from the Ponemon Institute showing that the average expense for a data breach in 2019 was $3.92 million. These immense expenses alone are a great motivation for health organizations to make the ransom payment if it is the cheaper option. In addition to monetary worries, health providers are sometimes coerced to make the ransom payments due to having their systems locked down. If the malware prevents electronic communications or access to the medical record systems, organizations may go ahead and make the payment in order to get the decryption key and restore access to its systems. Being unable to access the medical records system for one day could seriously damage a hospital's reputation (Solander, Forman & Glasser, 2016).

A third significant reason the healthcare industry experiences so many ransomware attacks is the increased exposure due to devices known as the Internet of Things (IoT) and Internet of Medical Things (IoMT). These advanced medical machines have created more end points for hackers to target sensitive health data (Lee & Jackson, 2018). IoT devices are used in healthcare settings for purposes such as remote monitoring of patients, administration of medications and tracking hospital bed occupancy. IoMT devices are the medical version of IoT devices and, as previously explained, are mobile healthcare devices which can provide remote monitoring, even from a patient's home. The issue with IoT and IoMT devices in relation to cyberattacks is that these devices are generally less secure than regular computers and are not easily updated. Therefore, they are more vulnerable to attack. When criminals hack into these devices, they are able to watch network traffic, steal passwords and confidential data (Abraham, Chatterjee & Sims, 2019). Another issue with IoMT devices is that general security mechanisms aimed at detecting attacks are not compatible with the devices. These devices are different from regular computers due to the nature of their mobility. Their features, which include computing power, memory space, battery life and network bandwidth, do not mesh well with current security mechanisms (Kumar, Gupta & Tripathi, 2020).

A fourth reason the healthcare industry is threatened with increased cyberattacks is that while healthcare professionals are expertly trained in their particular field, they are generally not well-educated on cybersecurity awareness. In a survey conducted in 2015 by the Health Information and Management Systems Society, 64% of respondents had encountered a security incident in their organization due to phishing. Phishing emails are designed to look like a legitimate email but contain attached files, which launch a piece of ransomware when opened (Harkins & Freed, 2018). Based on multiple works of research, phishing emails are the typical method used by criminals to deliver malicious links and malware (Pagán & Elleithy, 2021). According to a report published by Zimba & Chishimba (2018) and referenced in Figure 1, 31% of ransomware attacks in 2016 came through email links, while 28% of attacks were launched through email attachments. Together these account for almost 60% of all ransomware infections. Due to the fact that healthcare employees interact with the public on a daily basis, they may be used to opening emails from unknown sources (Solander, Forman & Glasser, 2016). In addition, some of the email messages healthcare employees receive may be spoofed so that they appear to be coming from a legitimate source, such as Lab Corp. These emails and attachments, which may be entitled "Patient Results" can contain malware and once opened can infect the organizations file system. If employees are not trained to spot these fraudulent emails, the computer systems could be at risk (Solander, Forman & Glasser, 2016).

Figure 1: *Various Avenues of Ransomware Attacks*



Note. From "On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems" by Zimba & Chishimba, 2018, *European Journal for Security Research*, *4*(1), 3–31.

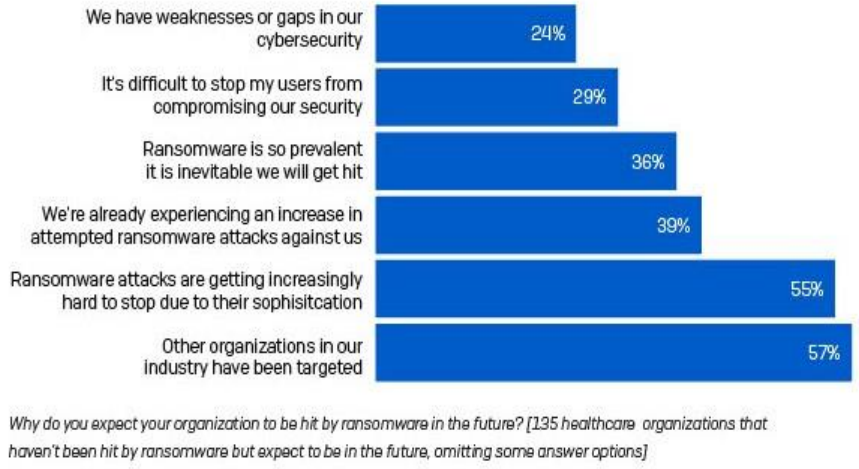
Finally, healthcare organizations are at risk for ransomware attacks due to insufficient information technology (IT) or cybersecurity protection. According to Chung (2019), many healthcare providers are using old systems and applications due to tight budgets and minimal information security allowances. As David T. Jamison, executive director of the Health Devices Group at the ECRI Institute stated, "Patient safety is on everyone's mind, but technology safety sometimes gets left behind" ("Ransomware and Other Cybersecurity", 2017). As an example of aging technology in the healthcare field, Chinthapalli (2017) reported that 90% of England's NHS Trust's computers in 2017 used Windows XP, which was already obsolete by that year. At the same time health care systems are aging, ransomware techniques are advancing. Chung (2020) advised that health care providers still using traditional security methods such as antivirus, firewalls, and intrusion detection systems (IDS) are leaving the organizations open to attacks. Bobrow (2021) took this a step further claiming that quantitative risk analysis, which is a vital way to assess cybersecurity, is currently missing from most security programs. Adding to these issues are vulnerabilities created in computer systems when healthcare organizations merge. When the two systems join, IT challenges arise and potentially leave areas open to attack (Lee & Jackson, 2018).

In addition to protecting in-house computers, healthcare organizations must also think about security protection for their web and cloud servers. These are popular targets for hackers because they contain sensitive data and have strong CPUs that criminals can use for crypto mining. In addition, servers are rarely shut down since they must be readily available, so these machines are rarely analyzed (Or-Meir et al., 2019). Adding to the complexity of the issue, some healthcare organizations use 3rd party service providers for their cloud-based storage. In this case, it is hard for companies to ensure that these service providers will take the steps necessary to protect their sensitive data (Abraham, Chatterjee & Sims, 2019).

While cybersecurity protection is often lacking in healthcare organizations, hackers are focusing on making ransomware attacks even more advanced. Criminals no longer need physical contact with hospital systems to launch a cyberattack as they now have virtual attack options. As referenced in Figure 2, Sophos reported that 55% of healthcare professionals surveyed agreed that ransomware attacks are increasing in sophistication and becoming harder to stop ("The State of Ransomware", 2021). One creative hacker breached a hospitals IT system by breaking in through their food services network. Once inside, they were able to gain access to health records (Lee & Jackson, 2018). Other cyber criminals

prefer traditional routes such as phishing emails or more innovative approaches through medical devices such as IoMTs (McLarren, 2018). While it might seem that increasing IT security would be the apparent solution to reducing the number of cyberattacks, many CEOs and CFOs are hesitant to do so because there is minimal return in increased financial stability (Lee & Jackson, 2018).

Figure 2: *Why Healthcare Expects to be Hit*



Note. From "The State of Ransomware in Healthcare 2021" by Sophos, 2021, Retrieved June 6, 2021 (https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf)

Dilemmas Created by Ransomware Attacks

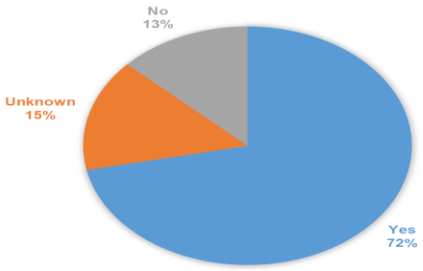
When healthcare organizations experience a ransomware attack, they face many dilemmas. In 2016, when the Hollywood Presbyterian Medical Center located in Los Angeles experienced an attack, secretaries could not access their emails, doctors could not access electronic health records and computerized tomography scans could not be done. The CEO announced they had an emergency and ambulances were diverted to other hospitals (Chinthapalli, 2017). Unfortunately, when this happens, healthcare organizations are at the mercy of the attackers. The criminals, knowing they have the upper hand, give the organization an option to pay or permanently forfeit access to all patient data (McLarren, 2018). However, this decision is a very complex one with many potential ramifications.

First, if a healthcare organization chooses to make the ransom payment in hopes of having their services restored, they can be in violation of U.S. law and subject to civil penalties. The Office of Foreign Asset

Control (OFAC) has sanctioned many cybercriminals so payment to them may leave the healthcare organization in legal turmoil. In addition to that dilemma, even with payment made, there is no guarantee that all patient information will be returned. Depending on the type of malware used, versions such as NotPetya encrypts the computers' master boot records and cannot be reversed. Therefore, even if a ransom payment is made, the machines cannot be restored (Garrie & Halprin, 2021). In fact, according to a survey that Vanson Bourne, an independent research house, conducted on behalf of Sophos, only 69% of captured data was fully returned after a ransom payment was made ("The State of Ransomware", 2021).

Second, if a healthcare provider chooses not to make the ransom payment, the healthcare organization may end up in violation of the Health Insurance Portability and Accountability Act (HIPAA) protocols. According to Bertheau (2021), advanced ransomware tactics now employ a double extortion where they extract patient data prior to locking up the computer systems. Therefore, they can threaten to release the sensitive patient health information, forcing the healthcare system to be in violation of HIPAA if they do not pay (Bertheau, 2021). This is the situation San Diego-based Scripps Health found itself in as data from almost 150,000 patients was stolen prior to deploying ransomware (Landi, 2021). So far this year, 72% of ransomware incidents resulted with victim data leaked, according to the "Ransomware Trends 2021" study by the Department of Health and Human Services, as referenced in Figure 3. This is particularly troubling for healthcare centers trying to follow all legal protocol. As McLarren (2018) explains, in 2016 the HHS Office of Civil Rights (OCR) stated that unless a hospital can prove via four different criteria that a breech did not occur, it will be presumed that one did happen. Data breaches have become very common in the U.S. with 91% of all health organizations reporting one between 2016-2018 (McLarren, 2018). In addition to violating HIPAA laws, leaked patient information may result in negative press and damaged reputation for the healthcare organization.

Figure 3: *Ransomware Incidents Resulting in Data Leaked*



Note. Data compiled from January – May 2021.

U.S. Department of Health and Human Services. (2021). *Ransomware Trends 2021*. HHS Cybersecurity Program (https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf)

Financial and Public Health Implications

When it comes to ransomware attacks on healthcare providers, there are major implications no matter which decisions the organization has made with the dilemmas provided. These ramifications are so significant that Kapersky Lab has declared ransomware as the third most serious threat to small and medium size companies (Mansfield-Devine, 2016). In fact, in 2019, a healthcare private practice in Battle Creek, Michigan was forced out of business after a ransomware attack. This is the first public report of a business failure due to ransomware (Chung, 2019). When it comes to cyber-attacks on healthcare providers, there are major implications in the areas of financial loss and diminished standards of patient care.

One of the most extensive costs included in a ransomware attack is that of financial loss. The most apparent cost is the ransom payment itself, if the company chooses to pay it. According to Chung (2020), the average payout increased by 6 times between 2018 and 2019 to $41,198. Ever increasing, the HC3 organization created by the Department of Health and Human Services marked the average ransom payment by healthcare providers during the first five months of 2021 as $131,000 (“Ransomware Trends”, 2021). Whether a company chooses to pay the ransom payment or not, they will surely incur losses due to downtime and recovery efforts. According to Zimba & Chishimba (2019), these costs vary from thousands to millions of dollars, especially if they do not have backups for their data. In the recovery process, mitigation for a healthcare provider could include restoration of affected computers, email communication blackout, rebuilding computer service, discounted or free services to patients affected and strengthening the security infrastructure. In 2017, the health company Merck was attacked with by a vicious ransomware software known at

NotPetya. The ransom demand was only $50,000 but the recovery cost was estimated at $310 million (Zimba & Chishimba, 2019).

Unfortunately, even healthcare companies who rely on cyber insurance policies to fully reimburse any ransomware expenses may experience severe financial losses. If the organization does not clearly understand the exclusions and exceptions of the policy, they may be surprised to find out what is not covered. In 2018, Mondelez International, Inc. tried to cash in its insurance policy with Zurich American Insurance Company after a vicious ransomware attack. However, instead of payment the business was notified that it was denied coverage due to a war exclusion. Apparently, the exclusion was based on a "hostile or warlike action" (Garrie & Halprin, 2021, p. 16).

Another implication of ransomware attacks on the healthcare industry is the compromised care of patients. According to Steve Mansfield-Devine (2016), editor of *Network Security*, many hospitals have been attacked globally. When this happens and critical systems are down, lives could be in danger (Mansfield-Devine, 2016). In the *Journal of Health Care Compliance,* the ECRI Institute, listed the "patient safety component of ransomware and cybersecurity threats" as the No. 1 Health Technology Hazard ("Ransomware and Other Cybersecurity", 2017). Harkins & Freed (2018) echo this thought stating a ransomware attack on a health care center has a higher price than money paid for ransom. In fact, these attacks have proven to delay patient care and potentially lead to loss of life. In 2017, a ransomware attack was launched on forty hospitals in the U.K.'s National Health Service network. Due to the attack, surgeries and medical appointments were reportedly canceled and lab results were delayed (Harkins & Freed, 2018). Marty Edwards, director of Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team warned, "It's only a matter of time before we see some sort of significant type of events that involve patient safety that are cyber enabled" (McLarren, 2018).

Discussion to Minimize Ransomware Risks

Ransomware attacks are prevalent in the healthcare industry to the extent that serious thought must be considered on how to minimize the risk. FBI Director, Robert Mueller, once stated that there are two kinds of organizations – ones that have faced a cyber-attack and ones that will face it (Pagán & Elleithy, 2021).

Table 1
Preparing for a Ransomware Attack

Preparation Areas	Steps to Minimize Risk
Network Security	Train employees on cybersecurity threats Address vulnerable network areas Upgrade computer systems Create offensive cybersecurity plan Backup information frequently
Emergency Plan	Create business continuity plan Equip staff with proper tools and training Retain incident response team
Cyber Insurance Policy	Carefully review available policies Purchase extensive plan with reliable coverage

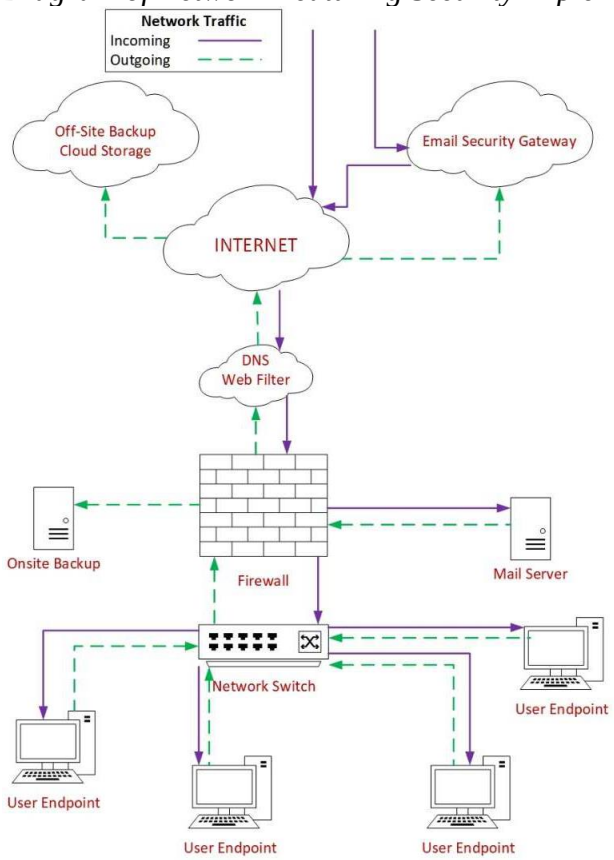
Although each healthcare provider has a unique situation, all can benefit from preventative planning through upgrading security, developing an emergency plan and investing in a trusted cyber insurance policy. A summary of the preparation steps for each of these aspects is presented in Table 1.

The first step in reducing the amount of risk a healthcare provider faces in a cyber-attack is to upgrade all facets of security. Pagán & Elleithy (2021) propose a multi-layered approach, beginning with employee training. Each person interacting with a computer in the facility should know how to recognize malicious emails, attachments or links and also be cognizant of the possible areas of infection. This investment alone should reduce the number of infections due to phishing emails. In addition to employee training, each healthcare provider should work though a risk assessment and penetration probe to discover the weak areas in their networks. Once found, the network needs to be checked to see if it can correctly isolate an infection (Solander, Forman & Glasser, 2016). With the vulnerable areas identified, healthcare providers should strongly consider upgrading all of their computer systems with advanced software such as antimalware protection (which signals when a possible infection is found), a firewall (which blocks common trapdoors and IP addresses), and a DNS/Web filter (which allows external requests to be checked and deemed safe before being connected) (Pagán & Elleithy, 2021). To bolster the protective layer even further, healthcare organizations should also work closely with a security employee or advisor to create an offensive cybersecurity plan.

This strategy should be robust enough to ensure their company is out of harm's way and is effective in keeping them from experiencing a data breach (Chung, 2020). Finally, in order to reduce the amount of risk of data loss in an attack, organizations would be wise to commence thorough and frequent backup procedures for all impertinent and sensitive information (Solander, Forman & Glasser, 2016). In addition, the HC3 organization recommends the 3-2-1 Backup Rule. This strategy includes keeping three copies of data at two separate locations and making sure at least one copy is stored off site ("Ransomware Trends", 2021). Along with that tip, when setting up the backup procedure, healthcare providers might consider using tape drives, which cannot be breached digitally (Chinthapalli, 2017). An example of a network diagram with many of these security features is shown in Figure 4 (Pagán & Elleithy, 2021).

Figure 4

Diagram of Network Featuring Security Implementations



Note. From "A Multi-Layered Defense Approach to Safeguard Against Ransomware" by Pagán, A., & Elleithy, K., 2021, *2021 IEEE 11th*

Annual Computing and Communication Workshop and Conference (CCWC), Computing and Communication Workshop and Conference (CCWC), 2021 IEEE 11th Annual, 0942–0947. https://doi-org.ezproxy.shsu.edu/10.1109/CCWC51732.2021.9375988

When developing an emergency plan, the Joint Security Advisory comprised of the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) suggest working through business continuity strategies. By having a plan in place and practicing it, essential business functions can continue, even though an emergency ("Ransomware Activity Targeting", 2020). When reviewing the emergency plan, organizations should ensure it includes policies, processes and expectations that would be followed in event of a cyber-attack. In addition, this plan should ensure the appropriate staff is in place and they are equipped with the proper tools and training to do their work (Lee & Jackson, 2018). Along with the plan, Bertheau (2021) recommends retaining a third-party response team ahead of time, which would respond in event of a ransomware attack. A good incident response team would be able to minimize the damage to the organization's reputation. In addition, they should take into account all contractual, legal and regulatory responsibilities as they relate to breach notifications. Also, if considering making a ransomware payment, organizations should first check to see if the criminals are on any of the OFAC lists, in order to avoid legal ramifications. Having open communication with law enforcement is significant in preventing issues with OFAC (Garrie & Halprin, 2021).

After upgrading security aspects and creating a robust emergency plan, organizations should also strongly consider investing in a cyber insurance plan. Although policies differ, Limmroth (2020) notes that some provisions include crisis management and communication, legal assistance, forensic inspection, and organization downtime analysis and reimbursement. By having a healthy cyber insurance plan, a team of experts will be deployed to handle the complex and delicate process. In addition, cyber insurance policies can cover costs such as crisis management, breach notification, regulatory defense, cost of data recovery, loss of business income, losses due to compromised email, losses due to damaged cell phones, and payment of ransom demand (if deemed necessary). All of these costs can be quite significant for an organization to pay during and after an attack. As previously mentioned, it is imperative that healthcare providers carefully read through any policy and ensure that they understand what is

and is not covered. This especially applies to any wording about a "war exclusion."

By exercising preventive planning through upgrading security, creating and testing an emergency plan, and purchasing a strong cyber insurance policy, healthcare organizations will be prepared for the inevitable ransomware attack.

Conclusion

In summary, ransomware attacks are widespread throughout the healthcare industry. These incidents are very significant as they threaten to disrupt and potentially harm the industry. Due to this issue, many in-depth studies have been done to research the problem and seek potential solutions. There are many indications of why the healthcare industry is specifically attacked, including the fact that they are easy targets and maintain sensitive information, which can be very lucrative for criminals. Once a ransomware attack is committed on a healthcare organization, it causes moral, ethical and legal dilemmas for the healthcare provider. These decisions must be carefully weighed out as the potential ramifications are extensive. When a cyber-attack is unleashed on a healthcare organization, it can result in substantial financial costs for the business and interruptions in medical care for the patients. In any case of ransomware attack, the potential for full recovery of data and computer systems may be slim depending on the type of malware used in the attack.

While preventative planning for healthcare providers is costly and extensive, the risk of not preparing is even more dangerous. Healthcare organizations should acknowledge that ransomware attacks are inevitable and strive to be prepared. As the threat of cyber-attacks continues to grow, healthcare organizations can create offensive strategies to combat the vicious attacks. With these efforts in place, the healthcare industry will reduce their vulnerabilities and will no longer be recognized as an easy target for criminals.

References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. https://doi-org.ezproxy.shsu.edu/10.1016/j.bushor.2019.03.010

Bertheau, C. (2021). The Ransomware Deluge: How to Navigate the Perfect Storm. *Plans & Trusts*, *39*(2), 16–21.

Bobrow, A. (2021). Quantifying Risk: Innovative Approaches to Cybersecurity. *German Marshall Fund of the United States*.

Retrieved June 9, 2021, from http://www.jstor.org/stable/resrep31797

Burde, Howard JD. (2011). The HITECH Act: An Overview. *Virtual Mentor*. 2011;13(3):172-175. doi: 10.1001/virtualmentor.2011.13.3.hlaw1-1103.

Chinthapalli, K. (2017). The hackers holding hospitals to ransom. *BMJ: British Medical Journal*, *357*. Retrieved June 4, 2021, from https://www.jstor.org/stable/26944485

Chung, M. (2020). New Ransomware Innovations Bring Shame and Fear to Health Care. *Journal of Health Care Compliance*, *22*(5), 37–63.

Chung, M. (2019). Taking Health Care Out of the Ransomware Hot Seat. *Journal of Health Care Compliance*, *21*(5), 53–54.

Federal Bureau of Investigation Cyber Division. (2014). Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain. Retrieved from http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

Garrie, D., & Halprin, P. A. (2020). Placing Ransomware in Context and Avoiding Liability for Paying Ransomware Claims. *Journal of Internet Law*, *24*(5), 1–19.

Harkins, M., & Freed, A. (2018). The Ransomware Assault on the Healthcare Sector. *Journal of Law & Cyber Warfare*, *6*(2), 148-164. Retrieved June 4, 2021, from http://www.jstor.org/stable/26441292

Joint Cybersecurity Advisory. (2020). Ransomware Activity Targeting the Healthcare and Public Health Sector. Retrieved from https://www.aha.org/system/files/media/file/2020/10/joint-cybersecurity-advisory-aa20-302a-ransomware-activity-targeting-hph-sector-10-28-20.pdf

Kumar, P., Gupta, G. P., & Tripathi, R. (2021). An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. *Computer Communications*, *166*, 110–124. https://doi-org.ezproxy.shsu.edu/10.1016/j.comcom.2020.12.003

Landi, H. (2021). Before attacking IT systems, hackers stole information from 147K patients, Scripps Health says. *FierceHealthcare*, N.PAG.

Lee, D., & Jackson, J. (2018). Protecting Against Cybersecurity Threats. *Hfm (Healthcare Financial Management)*, 1–4.

Limmroth, S. (2020). Cyber Insurance: An Insider's Guide to Why You Should Have Coverage. *Journal of Health Care Compliance*, *22*(3), 51–69.

Mansfield-Devine, S. (2016). Ransomware: taking businesses hostage. *Network Security*, *2016*(10), 8–17. https://doi-org.ezproxy.shsu.edu/10.1016/S1353-4858(16)30096-4

McLarren, C. (2018). Once More Unto the Breach: How the Growing Threat of Ransomware Affects Hipaa Compliance for Covered Entities. *Indiana Health Law Review*, *15*(2), 305–330. https://doi-org.ezproxy.shsu.edu/10.18060/3911.0051

Nicol, D. (2021). The Ransomware Threat to Energy-Delivery Systems. *IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Secur. Privacy*, *19*(3), 24–32. https://doi-org.ezproxy.shsu.edu/10.1109/MSEC.2021.3063678

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic Malware Analysis in the Modern Era--A State of the Art Survey. *ACM Computing Surveys*, *52*(5), 1–48. https://doi-org.ezproxy.shsu.edu/10.1145/3329786

Pagán, A., & Elleithy, K. (2021). A Multi-Layered Defense Approach to Safeguard Against Ransomware. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Computing and Communication Workshop and Conference (CCWC), 2021 IEEE 11th Annual*, 0942–0947. https://doi-org.ezproxy.shsu.edu/10.1109/CCWC51732.2021.9375988

Ransomware and Other Cybersecurity Threats Top ECRI Institute's Annual Health Technology Hazards List: Top 10 List Includes Endoscope Reprocessing Failures, Contamination Issues, and Missed Alarms. (2017). *Journal of Health Care Compliance*, *19*(6), 39–40.

Solander, A. C., Forman, A. S., & Glasser, N. M. (2016). Ransomware--Give Me Back My Files! *Employee Relations Law Journal*, *42*(2), 53–55.

Sophos. (2021). The State of Ransomware in Healthcare 2021. Retrieved June 6, 2021, from https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf

Statista. (2021). Share of U.S. organizations that experienced a ransomware attack and paid ransom 2020. Retrieved from https://www-statista-com.ezproxy.shsu.edu/statistics/701282/ransomware-experience-of-companies/

U.S. Department of Health and Human Services. (2021). *Ransomware Trends 2021*. HHS Cybersecurity Program. Retrieved from

https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf

Zimba, A., & Chishimba, M. (2019). On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *European Journal for Security Research*, *4*(1), 3–31.

Journal of Business and Accounting
Vol 14, No 1; Fall 2021

INVESTOR DISTRACTION AND INTERTEMPORAL VARIATION IN THE NUMBER OF EARNINGS ANNOUNCEMENTS: A TRADING VOLUME ANALYSIS

Ivo Ph. Jansen
Andrei L. Nikiforov
Rutgers, The State University of New Jersey
Lee W. Sanning
Colorado State University

ABSTRACT

Prior research shows that investors get distracted in the presence of information overload, and several studies have used the number of daily earnings announcements as a proxy for information arrival. We document, however, that investor attention to a firm's earning announcement—as proxied by abnormal trading volume in that stock—does not display a uniformly negative relation with the market-wide number of earnings announcements. Specifically, we show that while many more firms announce their earnings just outside of the trading day than during the trading day, those announcements nonetheless receive a lot more attention. We also show that while relatively few firms announce their earnings just after the market closes on Fridays, those announcements nonetheless receive very little attention. This study thus provides important evidence to reconsider the usefulness of the number of earnings announcements as an indicator of investor distraction. In addition, it refines the corresponding advice to managers who wish to time their earnings announcements to receive more or less attention.

Key Words: Earnings Announcements, Strategic Timing, Investor Distraction, Abnormal Trading Volume

INTRODUCTION

This study is an extension of Jansen, Nikiforov and Sanning, 2020 (hereafter JNS 2020) on the very pronounced intertemporal variation in the number of earnings announcements during the weeks in a quarter, days of the week, and times of day. JNS 2020 reviews literature which shows that investors become distracted in the presence of information overload and therefore present their results to assist managers in determining (1) when an earnings announcement would be "competing" with more or fewer earnings announcements and, by extension, (2) when it would be receiving more or less investor attention. In this study, we extend JNS 2020 to investigate how a firm's abnormal trading volume around its earnings announcements varies as a function of the intertemporal variation in the market-wide number of earnings announcements.

Implicit in JNS 2020, and based on the literature they review on investor distraction and information overload (e.g., Hirshleifer et al., 2009, and DeHaan et al., 2015), is the argument that investors become more distracted as the number of earnings announcements increases. This study explicitly investigates that argument using a firm's abnormal trading volume at the time of its earnings announcement as a proxy for investor attention to that announcement. Our results show that, on a weekly level, there is a strong negative relation between average abnormal trading volume and the market-wide number of firms announcing their earnings, consistent with the idea that information overload causes investor distraction. However, looking at more narrow windows, this relation is either absent or directly opposite. For example, when looking within a day, most firms announce their earnings either just before the market opens (39%) or just after it closes (50%), whereas very few firms announce their earnings during the trading day (4%). At face value, Hirshleifer et al.'s (2009) investor distraction hypothesis thus would predict that the announcements made during the day would, on average, receive the most attention, and that those made just outside of trading hours would receive the least attention. We document, however, the exact opposite, with announcements made by firms just outside of trading hours having more than double the amount of abnormal trading volume than those firms who made their announcement during the trading day. We speculate that the very low trading volume for during-the-day announcements is due to investors being pre-occupied with the analysis of market data during the trading day. In that sense, the low trading volume for these during-the-day announcements would still be due to distraction, but not because of the arrival of other *fundamental* information such as earnings news, but because of investors' focus on trading activities and the arrival of market data during the trading day.

We conclude, therefore, that intertemporal variation in the number of firms announcing their earnings is, at best, a flawed indicator of investor attention. It does appear to be useful to assess investor attention from week to week, but not from day to day, or within a day. Indeed, it appears that many other factors besides fundamental information distract investors. There is evidence in prior research which shows that those factors include Fridays and the upcoming weekend (DellaVigna and Pollet, 2009) religious Holidays (Pantzalis and Ucar, 2014) and the World Cup soccer (Ehrmann and Jansen, 2017). Our study suggests that investors' trading activities during the day, and trading data that arrives during the day, are additional factors to cause investor distraction. As far as our advice to managers to assist them in timing their earnings announcements, we can clearly say, however, that announcements made during the trading day receive less attention, and that those made after trading ends on Friday receive the least attention of all.

PROXY FOR INVESTOR ATTENTION

We use abnormal trading volume as our measure of investor attention. An alternative measure used in some research is the abnormal return around earnings

announcements (see, e.g., Hirshleifer et al., 2009). We choose trading volume, however, for two reasons. First and foremost, trading volume reflects the *sum of trading activities* in a firm's stock from all investors around an information event, whereas returns reflect the *average belief revision about the value impact* of that event across all investors. As a result, if there is an information event that draws a lot of trading activity (i.e., individual investors who revise their beliefs about value) but where the *average* belief revision across investors is close to zero, trading volume would be high but the returns would be insignificant. Trading volume, in other words, is a much more sensitive measure of investor attention. Second, prices are subject to well-documented biases such as underreaction (e.g., Bernard and Thomas, 1989, 1990) and overreaction (e.g., Zarowin 1989; Jegadeesh and Titman, 1993). No such biases have been documented for trading volume.

We measure abnormal trading volume for a stock on the day of its earnings announcement as follows. First, we measure trading volume as daily shares traded divided by shares outstanding (i.e., share turnover). Next, because trading volume data is highly skewed, we use a log transformation of volume, consistent with prior research (e.g., Ajinkya and Jain, 1989; Campbell and Wasley, 1996). Finally, we compute abnormal trading volume for a given stock by subtracting, from raw volume, the average trading volume in that stock over the 30 trading-day period ending 11 days before the earnings announcement. We identify the earnings announcement day as the date *of* the announcement if it is made either before or during trading hours that day, and as the next trading date for announcements made after trading hours.

DATA

We obtain quarterly earnings announcement dates, and the exact time of the announcement, from the Institutional Broker's Estimate System (IBES). We define the first week of the year as the 7-day period starting on January 1, to maintain consistency across the years. We also split the sample by day of the week, and time of day: overnight (12am-6am), before trading (6am-9:30am), trading day (9:30am-4pm), after trading (4pm-6pm), and evening (6pm-12am). We obtain all 77,781 quarterly earnings announcements from IBES during the five years from 2014-2018. We obtain daily trading volume data from CRSP.

RESULTS

The first three figures relate abnormal trading volume (on the right axis) to the number of earnings announcements (left axis) across different time intervals (x-axis). Figure 1 does so for weeks during the year. The number of earnings announcements (left axis) represents the percentage of publicly traded firms announcing their quarterly earnings during that particular week. Abnormal volume is measured as the deviation from normal volume, with a value of 1 indicating that volume is 100% above normal. JNS 2020 already documented the pronounced

variation in earnings announcements during the year, with as many as 30% of firms announcing their earnings during the peak week of earnings season.

Figure 1: Average Abnormal Trading Volume and Earnings Announcements by Week

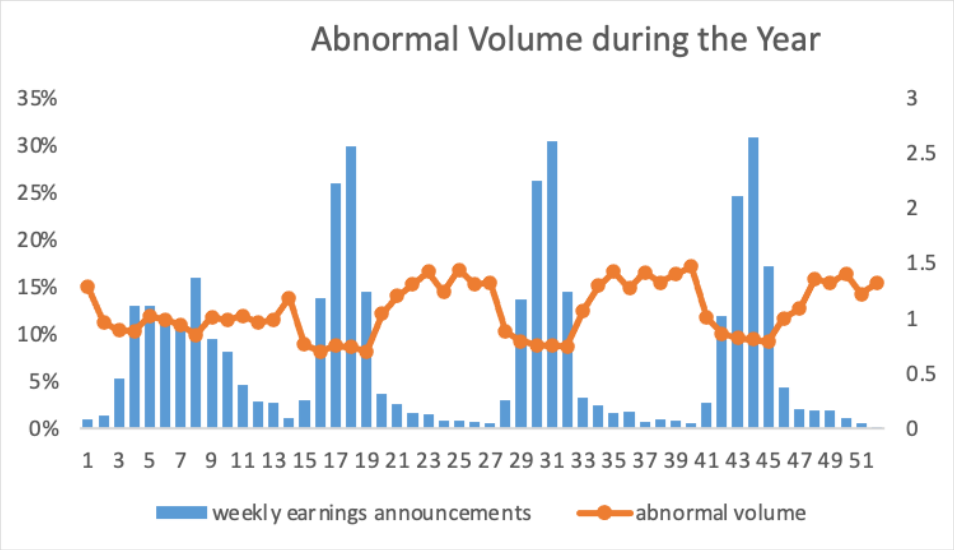


Figure 1 shows the percent of quarterly earnings announcements made during each week of the year (left axis), and the average abnormal trading volume per announcement (right axis). The sample consists of all 77,756 quarterly earnings announcements for the years 2014-2018 reported on IBES. Week 1 starts on January 1 and ends on January 7, etc.

Figure 1 shows that as the market-wide number of earnings announcements increases, the average abnormal trading volume for a firm announcing their earnings decreases, and vice versa. This result is observable throughout the year, and the correlation across the 52 weekly observations is -0.83. Figure 1 thus provides strong evidence in support of the argument that the weekly number of earnings announcements is highly indicative of investors being distracted by the number of other firms also announcing their earnings.

Figure 2 relates average abnormal trading volume to the number of earnings announcements across the days of the week. As already shown by JNS (2020), Thursday is the day with the most (32%), and Friday is the day with the fewest (7%) number of earnings announcements. Nonetheless, we find that abnormal trading volume is substantially lower on Friday than on other days, including Thursday. On a day-to-day basis, in other words, the number of earnings announcements is not a good indicator of investor attention at all. The Friday result in this figure is, however, consistent with DellaVigna and Pollet (2009), who show that stock prices tend to underreact to earnings announcements made on Friday.

They argue that on Friday investors are starting to focus on the upcoming weekend, and thus pay less attention to fundamental information like earnings news.

Figure 2: Average Abnormal Trading Volume and Earnings Announcements by Weekday

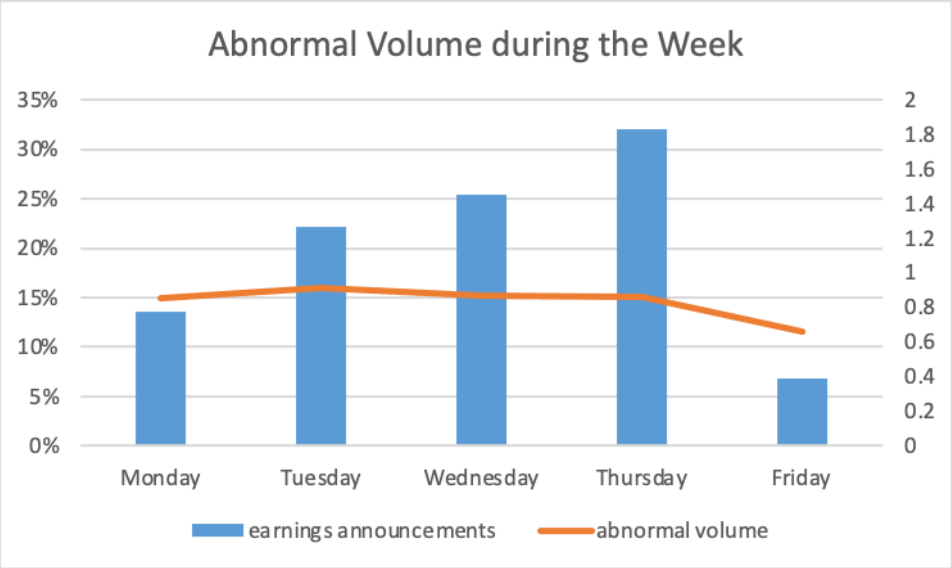


Figure 2 shows the percent of earnings announcements made by day of the week (left axis), and the average abnormal trading volume per announcement (right axis). The sample consists of all 77,756 quarterly earnings announcements for the years 2014-2018 reported on IBES.

Figure 3, next, relates average abnormal trading volume to the number of earnings announcements across the times of day. Note, first of all, that a large majority of firms announce their earnings either just before the trading day starts (39%) or just after it ends (50%), and that very few firms (4%) announce during the trading day (see also JNS, 2020). But also note that, despite there being very few announcements competing for investor attention during the trading day, the average abnormal trading volume for during-the-day announcements is much lower than it is for announcements made at other times.

Figure 3: Average Abnormal Trading Volume and Earnings Announcements by Time of Day

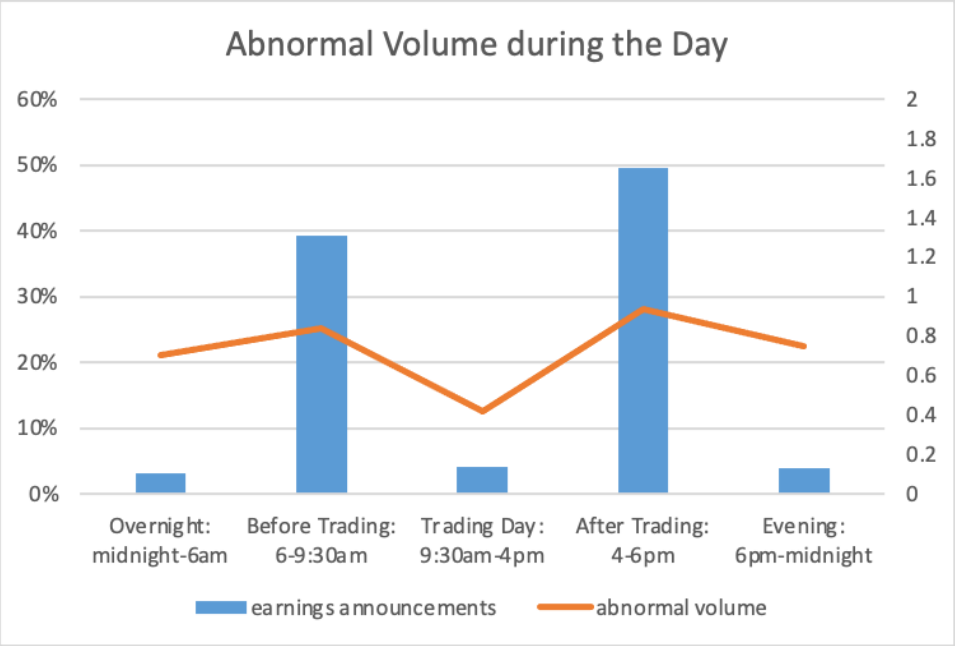


Figure 3 shows the percent of quarterly earnings announcements made at different times during the day (left axis), and the average abnormal trading volume per announcement (right axis). The sample consists of all 77,756 quarterly earnings announcements for the years 2014-2018 reported on IBES.

This seems to contradict the investor distraction hypothesis as developed by Hirshleifer et al. (2009), who indeed use the number of earnings announcements as their proxy for information arrival. Our view, however, is that it is not their hypothesis that is wrong, but that their proxy is too limited. Specifically, we think that investors may be getting distracted from processing earnings news during the trading day by their own trading activities, as well as by all the market/trading data that arrives during the trading day. In other words, we believe that distraction is real, but that there are many sources of distraction: not just fundamental news, but also market data, investors' own trading activities, as well as sources of distraction unrelated to investing (e.g., upcoming weekend social activities).

Figures 2 and 3 showed that Friday and during the day announcements, respectively, experience less abnormal trading volume. Figure 4, next, documents the *interaction* effect of day-of-the-week and time-of-day on abnormal trading volume. Figure 4 leaves out the number of earnings announcements to avoid cluttering.

Figure 4: Average Abnormal Trading Volume by Weekday and Time of Day

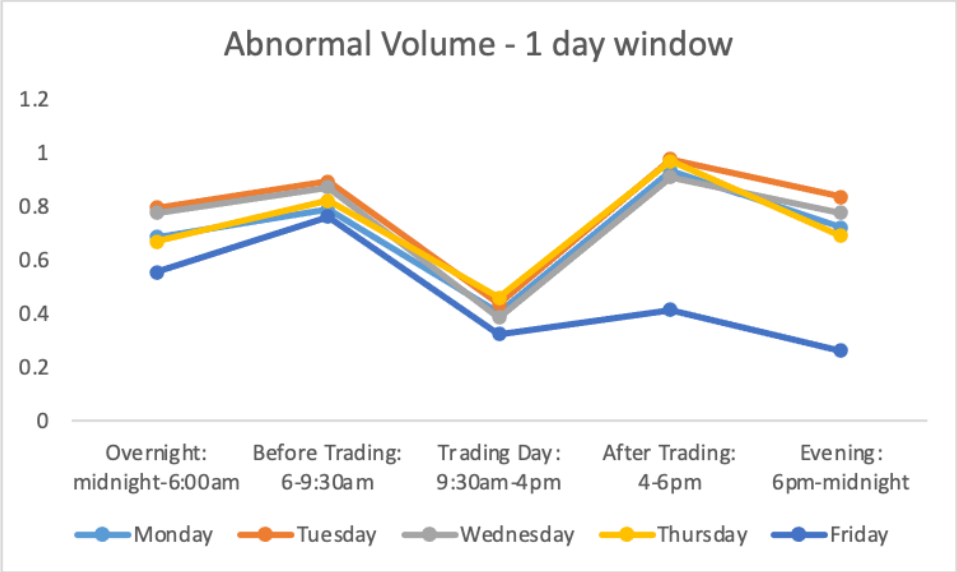


Figure 4 shows the average abnormal trading volume per announcement during different times of day and on different days during the week. The sample consists of all 77,756 quarterly earnings announcements for the years 2014-2018 reported on IBES.

Figure 4 shows that the intraday pattern from Figure 3 is nearly identical from Monday through Thursday. Friday, however, stands out. Specifically, Figure 4 shows that while the abnormal trading volume for announcements made either before or during the trading day is very similar to that on Monday through Thursday, the reason that Friday announcements experience less abnormal trading volume on average (see Figure 2), is almost entirely due to after-hours announcements. Figure 4 shows that announcements made on Fridays after the market closes receive much less attention than those made at other times. This finding is consistent with Michaely, Rubin and Vedrashko (2016), who show that some companies with bad earnings news seem to opportunistically shift their earnings announcement to occur after the market closes on Fridays.

Finally, Figure 5 replicates Figure 4 with one important modification in the measurement of abnormal trading volume to address a potential bias in our results thus. Specifically, abnormal trading volume for announcements made *during* the day may be lower simply because there is not a *full* trading day during which investors could respond to the announcement. (This obviously does not affect announcements made outside of the trading day.) We therefore decided to "bias the results in the opposite direction," by adding one *extra* day of abnormal volume for during-the-day announcers. Specifically, Figure 5 replicates Figure 4 using a *four*-day window for during-the-day announcers versus a *three*-day window for all others, where the first day in both cases is the day of the earnings

announcement. Figure 5 shows, however, that even in this case, there is still less abnormal trading volume for during-the-day announcers. Moreover, the overall pattern of Figure 4 remains. The potential bias noted above (for lack of a full day during which investors could respond to the announcement), therefore, does not seem to impact our results.

Figure 5: Average Abnormal Trading Volume by Weekday and Time of Day – Long Window

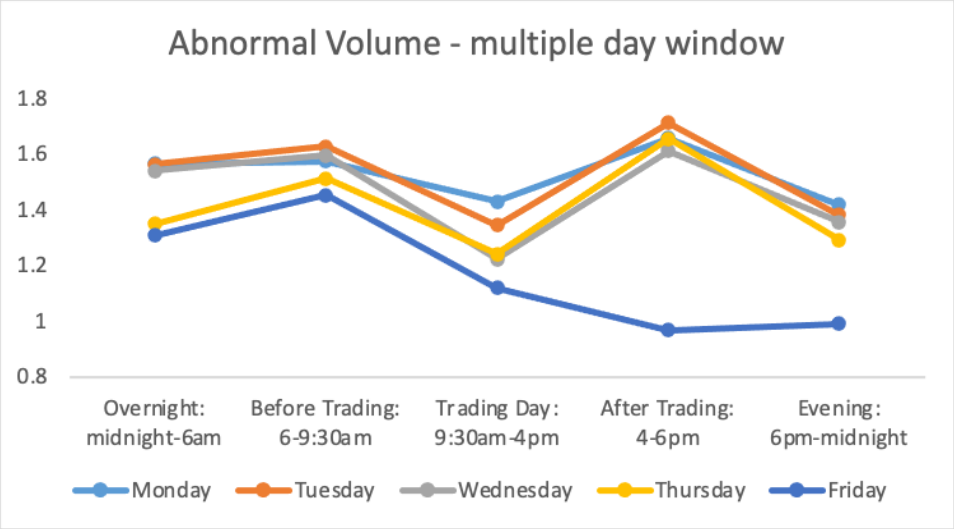


Figure 5 shows the average abnormal trading volume per announcement during different times of day and on different days during the week. The sample consists of all 77,756 quarterly earnings announcements for the years 2014-2018 reported on IBES. Abnormal trading volume is measured over a four-day window for during-the-day announcers, and over a three-day-window for all other announcements.

CONCLUSION

This study investigates the relation between abnormal trading volume and the number of earnings announcements across different time intervals. On a week-to-week basis, there is a strong negative relation: weeks with many earnings announcements are characterized by less abnormal trading volume per announcement, whereas weeks with few earnings announcements are characterized by more trading volume per announcement. This result is consistent with the number of earnings announcements being a useful indicator of investor distraction on a week-to-week basis.

Our analyses of shorter time-intervals, however, show a more complex picture. On days (Fridays in particular) or times of day (during the trading day in particular) when fewer firms announce their earnings, there is *less* trading volume

for the average announcement. Investor distraction, therefore, seems to be driven by more than just the number of earnings announcements alone (i.e., the arrival of fundamental information). Instead, it seems that the weekend, as well as investors' own trading activities and the arrival of market data, are important sources of distraction also.

This leads us to refine the advice in JNS (2020) to managers who wish to time their firm's earnings announcement to receive more or less attention. JNS (2020) advised managers who want to receive more investor attention to simply announce their firms' earnings at times when few others do, and vice versa. Based on this study's findings, however, we advise managers who wish to receive *more* investor attention to announce either just before the trading day begins or after the close of the trading day on Monday through Thursday. Moreover, we advise managers who wish to receive *less* investor attention to announce their firms' earnings on Fridays, either during or after the trading day.

REFERENCES

Ajinkya, Bipin, and Prem C. Jain, 1989. The behavior of daily stock market volume. Journal of Accounting and Economics 11 (November): 331–359.

Bernard, Victor L., and Jacob K. Thomas. "Post-earnings-announcement drift: delayed price response or risk premium?" *Journal of Accounting Research* 27 (1989): 1-36.

Bernard, Victor L., and Jacob K. Thomas, 1990. "Evidence that stock prices do not fully reflect the implications of current earnings for future earnings." *Journal of Accounting and Economics* 13 (4): 305-340.

Campbell, Cynthis J., and Charles J. Wasley, 1996. Measuring abnormal daily trading volume for samples of NYSE/ASE and NASDAQ securities using parametric and nonparametric test statistics. Review of Quantitative Finance and Accounting 6 (3): 309–326.

DeHaan, Ed, Terry Shevlin, and Jacob Thornock. "Market (in) attention and the strategic scheduling and timing of earnings announcements." *Journal of Accounting and Economics* 60, no. 1 (2015): 36-55.

DellaVigna, Stefano, and Joshua M. Pollet. "Investor inattention and Friday earnings announcements." *The Journal of Finance* 64, no. 2 (2009): 709-749.

Ehrmann, Michael, and David-Jan Jansen. "The pitch rather than the pit: investor inattention, trading activity, and FIFA World Cup matches." *Journal of Money, Credit and Banking* 49, no. 4 (2017): 807-821.

Hirshleifer, David, Sonya Seongyeon Lim, and Siew Hong Teoh. "Driven to distraction: Extraneous events and underreaction to earnings news." *The Journal of Finance* 64, no. 5 (2009): 2289-2325.

Jansen, Ivo, Andrei Nikiforov, and Lee W. Sanning. "Investor Distraction and Information Overload: Evidence to Help Managers Strategically Time Earnings Announcements." *Journal of Business and Accounting* 13, no. 1 (2020): 124-135.

Jegadeesh, Narasimham, and Sheridan Titman. "Returns to Buying Winners and Selling Losers: Implications for Stock Market Efficiency." *Journal of Finance*, vol. 48 (1993): 65–91.

Michaely, Roni, Amir Rubin, and Alexander Vedrashko. "Further evidence on the strategic timing of earnings news: Joint analysis of weekdays and times of day." *Journal of Accounting and Economics* 62, no. 1 (2016): 24-45.

Pantzalis, Christos, and Erdem Ucar. "Religious holidays, investor distraction, and earnings announcement effects." *Journal of Banking & Finance* 47 (2014): 102-117.

Zarowin, Paul. "Does the Stock Market Overreact to Corporate Earnings Information?" *Journal of Finance*, vol. 44 (1989): 1385–1399.

Journal of Business and Accounting
Vol 14, No 1; Fall 2021

THE CY 2021 PDGM 30-DAY HOME HEALTH PROSPECTIVE PAYMENT SYSTEM RATES FOR HOME HEALTH SERVICES

Gonzalo Rivera Jr.
Texas A&M University-Kingsville
Paul Holt
University of Central Oklahoma

ABSTRACT

The purpose of this paper is to discuss an overview of the new updated PDGM 30-Day Medicare HHPPS rates for CY 2021. For Medicare covered home health services beginning January 1, 2021, this finalized rule titled "Medicare and Medicaid Programs: CY 2021 Home Health Prospective Payment System Rate Update" discusses the new changes for the HHPPS payment rates. This proposed CY 2021 rule includes the current changes from the 60-day to the 30-day episode payment rates, and the national per-visit rates for home health services.

Key Words: Home health services; HHPPS; PDGM

HH PPS STANDARDIZED NATIONAL 60-DAY EPISODE RATE

Beginning October 1, 2000, as required by the Balanced Budget Act (BBA) of 1997 and its related amendments, BBA changed the way it reimbursed home health agencies for Medicare covered home health services using a new reimbursement method called the Home Health Prospective Payment System (HH PPS). Under HHPPS, all home health costs for Medicare covered services including medical supplies are paid using a basic unit of payment known as the 60-Day Episode. This HHPPS 60-day payment rate included the six home health service disciplines (skilled nursing, physical therapy, occupational therapy, speech therapy, home health aide, and medical social services). For home health services beginning October 1, 2000, Medicare computed the first HHPPS standardized national 60-day episode rate of $ 2,115.30 as presented by the following table (1) (HHPPS 1999).

FY 2000 Standardized National 60-Day Episode Payment Calculation (Table 1)

HHA discipline Type / Non-Routine Supplies (NRS)	Average cost per visit from PPS audit sample / Average cost per episode (NRS…)	Average number of visits for episodes with >4 visits from CY 98-episode file	HHA prospective payment rate
Skilled Nursing	$94.96	14.08	$1,337.00
Home Health Aide	$41.75	13.4	$559.45
Physical Therapy	$104.05	3.05	$317.35

Occupational Therapy	$104.76	.53	$55.52
Medical Social Service	$153.59	.32	$49.15
Speech Therapy	$113.26	.18	$20.39
NRS - cost report	$43.54		$43.54
NRS – Part B	$6.08		$6.08
Part B Therapies	$17.67		$17.67
Initial OASIS cost	$5.50		$5.50
Cont'd OASIS cost	$4.32		$4.32
			$2,416.01

Total non-standardized payment	Standardized factor - wage index & case-mix	Budget neutral-ity factor	Outliers adjust-ment factor	Final standardized 60-day episode rate Oct. 2000
$2,416.01	/ .96184	* .88423	/ 1.05	$2,115.30

The standardized 60-day episode payment rate was further updated for each of the next two (2) years (HHPPS 2001; HHPPS 2002).

MEDICARE PRESCRIPTION DRUG, IMPROVEMENT AND MODERNIZATION ACT OF 2003

The Medicare Prescription Drug, Improvement and Modernization Act of 2003(DIMA) updated the national home health standard prospective payment system (HHPPS) rates for 60-day episodes ending October 1, 2003-December 31, 2004 and the bill required updated payment increases to be computed on a calendar year basis beginning January 1, 2005. The following table (3) reflects the updated standardized 60-day episode rates that was required by the 2003 DIMA for the following periods 2003-2006 (Medicare Prescription 2003); (HHPPS 2004; 2005; 2006).

HHPPS NATIONAL 60-DAY EPISODE PAYMENT RATE FOR EPISODES BEGINNING IN CY 2008

For 60-day episodes beginning in 2008, the Medicare HHPPS national standardized rate was updated by a new 153 case mix grouping called home health resource groups (HHRGs) and a new wage index value was determined by the site of the home health services. The August 29, 2008 (72 FR 49792) and November 30, 2008 (72 FR 67656) Federal Registers discussed the new changes under the "Home Health Prospective Payment System Refinement and Rate Update For Calendar Year 2008" rule which included the adjustments to the rebasing and revising of the home health market basket, resulting in new labor portion percentage of 77.082 and non-labor portion percentage of 22.918; this rule updated the LUPA (Low Utilization Payment Adjustments) per-visit payment rate, and the inclusion of an new additional payment for NRS (Non-Routine Supplies) (HHPPS 2008). The following table

(2) reflects the calculations used to update the national standardized payment rate under the Medicare HHPPS for 60-day episodes beginning and ending CY 2008 (HHPPS 2008).

CY 2008 Medicare HHPPS National 60-Day Episode Standardized Payment Rate (Table 2)

CY 2007 National Standardized 60-day episode payment rate	Multiplied by the Home Health Market Update 3.0 percent	Multiplied by outlier adjusted national payment rate	Adjustments for LUPA, SCIC, NRS, Outliers, and 0.0275 reduction for case mix changes	HH PPS CY 2008 National 60-Day Standardized Episode Payment Rate
$ 2,339.00	X 1.030	X 1.05	-259.31	$ 2,270.32

WEIGHTS FOR NON-ROUTINE MEDICAL SUPPLIES (NRS)—SIX-GROUP APPROACH EFFECTIVE CY 2008

The Home Health Prospective Payment System Refinement and Rate Update for Calendar Year 2008 included an additional payment for Non-Routine Supplies (NRS). The NRS payment amounts were computed by multiplying the relative weight for a particular severity level by the NRS conversion factor. The NRS conversion factor was updated by the home health market basket update of 2.9 percent and reduced by the 2.75 percent reduction. The CY 2008 NRS conversion factor for was $52.35. The following table (3) computed the new additional payment for NRS (Non-Routine Supplies) incurred in home health services for CY 2008 60-day episodes. The additional payment amount was based on the severity level of the patient care (HHPPS 2008).

CY 2008 Additional Payment for NRS (Table 3)

Severity Level	Points Scoring	Relative Weight	Conversion Factor	Payment Amount
1	0	0.2698	$ 52.35	$ 14.12
2	1 – 14	0.9742	52.35	51.00
3	15-27	2.6712	52.35	139.84
4	28-48	3.9686	52.35	207.76
5	49-98	6.1198	52.35	320.37
6	99+	10.5254	52.35	551.00

HH PPS NATIONAL 30-DAY NATIONAL PAYMENT FOR EPISODES BEGINNING IN CY 2020

For home health services beginning January 1, 2020, the finalized rule titled "Medicare and Medicaid Programs; CY 2020 Home Health Prospective Payment System Rate Update "includes the new change from a 60-day episode to a 30-day episode unit of payment, and a new patient 432 HHRG case-mix grouping named Patient-Driven Groupings Model (PDGM) (HHPPS 2019). This new PDGM will determine LUPAs and eliminate the need for a separate NRS calculation. To calculate the CY 2021 30-day national standardized payment rate, the following adjustments were applied to the CY 2020 national standardized payment rate: wage index neutrality factor of 0.9999; and a home health payment update factor of 1.020. The following table (4) reflects the HHPPS national standardized 30-day episode payment rate for CY 2021 (HHPPS 2020).

CY 2020 30-Day Episode National Standardized Payment Amount
(Table 4)

CY 2020 30-Day Episode National Standardized Payment	Neutrality Factor Wage Index	HH CY 2021 Payment Update	CY 2021 30-Day Episode National Standardized Payment
$ 1.864.03	X .09999	X 1.020	$ 1.901.12

NATIONAL PER-VISIT PAYMENT AMOUNTS USED TO PAY LUPAS FOR CY 2021

The HHPPS 2020 finalized rule updated the national per-visit rate. This national per-visit rate is used in paying low- utilization payment adjustments (LUPAs). LUPAs are defined as 30-day episodes with four or fewer visits. The payment per- visit amount is based on the type of home health visit or home health service discipline. There are six home health (HH) disciplines as noted on Table 8 below. In determining the CY 2021 national per-visit amounts used for LUPA episodes, the CY 2020 per-visit amounts were calculated for each home health service discipline by the following adjustments: a wage index budget neutrality factor of 0.9997; and an updated 2020 HH payment update factor of 2.0 percent. The CY 2021 national per-visit rates for each HH discipline are shown below in Table 5 (HHPPS 2020).

CY 2021 National Per-Visit Home Health Discipline Type Payment (Table 5)

Home Health Discipline Type	Per-Visit Payment CY 2020	Neutrality Factor Wage Index	HH Payment Update CY 2020	Per-Visit Payment Amount CY 2021
Home Health Aide	$67.78	x .09997	x 1.020	$69.11
Medical Social Services	$239.92	x .09997	x 1.020	$244.64
Occupational Therapy	$164.74	x .09997	x 1.020	$167.98
Physical Therapy	$163.61	x .09997	x 1.020	$166.83
Skilled Nursing	$149.68	x .09997	x 1.020	$152.63
Speech Pathology	$177.84	x .09997	x 1.020	$181.34

LOW UTILIZATION PAYMENT ADJUSTMENT (LUPA) ADD-ON FACTORS CY 2021

The Table 5 per-visit rates computed above are before an additional payment is added to the LUPA payment. Beginning in CY 2021, home health agencies with LUPAs payments for episodes billed as the only episode or the initial episode are to be paid an additional amount (Add-on Factor). For CY 2021, the additional amount paid to LUPAs billed as initial episodes in a sequence of adjacent episodes or as the only episode is based on the following three factors: SN 1.8451; PT 1.6700; and SLP 1.6266 (HHPPS 2020).

COMPUTING THE CY 2021 HHPPS 30-DAY EPISODE PAYMENT RATE FOR A HOME HEALTH AGENCY

As stated in the Medicare HHPPS rules effective January 1, 2020, the new basic unit of payment is a 30-day episode national standardized rate. This standardized rate is adjusted for by a PDGM HHRG case-mix weight and a wage index value based on the site of service. To help account for geographical wage differences, a part of the wage index value is applied to a labor related portion and non-labor related portion. The example below demonstrates a sample computation using the national home health standardized prospective payment system (HHPPS) rates for the 30-day episodes beginning CY 2020. The example computation includes the CY 2021 PDGM case-mix weights for a city with the Core Based Statistical Area (CBSA) codes for labor wage indexes. The wage index is adjusted with the labor portion of 76.1 percent and the non-labor portion of 23.9 percent. The total 2021 HHPPS payment a community home health agency receives for providing Medicare covered services in Corpus Christi, Texas based on the information below amounts to $ 2,165.27.

	Corpus Christi, Texas
1. CBSA Number Site of Service (See Table 6)	18580
2. PDGM HHRG 1FC11 Case Mix Weight (See Table 7)	1.1798
3. 2021 National 30 Day PPS Rate (See Table 4)	$ 1,901.12
4. PDGM HHRG Weight 1FC11 (See Table 7)	1.1798
5. Case Mix Adjusted PPS (Line 3 * Line 4)	$ 2,242.94
6. Labor Rate Percentage	0.761
7. CBSA Labor Wage Index – 18580 (See Table 6)	0.9545
8. CBSA Labor Wage Adjusted Rate PPS (Line 5 * Line 6* Line 7)	$ 1,629.21
9. National PPS Rate -Non-Labor Rate %	0.239
10. Case Mix PPS Rate – Non-Labor Rate % (Line 5 * Line 9)	$ 536.06
11. Adjusted PPS Rate (Line 8 + Line 10)	$ 2,165.27

Medicare HHPPS CY 2021 Wage Index (Table 6) *

CBSA	Urban /Rural Area	CBSA Name	CY 2021 Wage Index
18580	Urban	Corpus Christi, Texas	0.9545
99945	Rural	Texas	.82.82.82 0.8211

HHPPS CY 2021 Case-Mix Weights (Table 7) *

CY 2021 PDGM LUPA THRESHOLD AND CASE MIX WEIGHT FOR EACH HHRG PAYMENT GROUP				
HIPPS	Clinical Group and Functional Level	Timing and Admission Source	Visit Threshold (10th percentile or 2 - whichever is higher)	CY 2021 Weights
1FC11	Behavioral Health - High	Early - Community	4	1.1798
1FC21	Behavioral Health - High	Early - Community	4	1.2305
1FC31	Behavioral Health - High	Early - Community	4	1.3271
2FC11	Behavioral Health - High	Early - Institutional	4	1.3599

* Medicare and Medicaid Programs; CY 2021 Home Health Prospective Payment System Rate Update.

CONCLUSION

Home health agency administrators, supervisors, and financial officers need to calculate and evaluate the Medicare HHPPS payment amounts expected to be received for each of their patients admitted for home health services. These financial administrators should prepare standardized payment tables for each of their sites of services. These tables should reflect the current HHPPS payment amount for a patient assigned a particular PDGM HHRG payment group within each of the 30-day episode based on the site of service. Under the CY 2021 HHPPS rule, home health agencies are to be reimbursed one total for all home health services, including routine and non-routine medical supplies, provided to their patients within each 30-day episode. Home health agencies need to calculate their per-patient costs for each type of home health service. By obtaining the per-patient cost for each of the different home health services, an agency will be able to determine the total number of visits financially feasible within the 30-day episode.

REFERENCES

Medicare Program. *Prospective Program Payment System for Home Health Agencies 1999*, 42 FR Vol. 64 Parts 409, 410, 411, 413, 424, and 484.

Medicare Program. *Update to the Prospective Program System for Home Health Agencies FY 2000, 2001*, F.R. Vol. 66, No. 126.

Medicare Program. *Update to the Prospective Program System for Home Health Agencies FY 2002,* F.R. Vol. 67, No. 125.

Medicare Program. *Medicare Prescription Drug, Improvement, and Modernization Act of 2003,* P.L.: 108-173, Section 701.

Medicare Program. *Home Health Prospective Payment System Rate Update for Calendar Year 2005*, FR Vol. 69, No. 204.

Medicare Program. *Home Health Prospective Payment System Rate Update for Calendar Year 2006*, FR Vol. 70, No. 216.

Medicare Program. *Home Health Prospective Payment System Rate Update for Calendar Year 2007*, FR Vol. 71, No. 149.

Medicare Program. *Home Health Prospective Payment System Refinement and Rate Update for Calendar Year 2008*, FR Vol. 72, No. 230.

Medicare Program *Home Health Prospective System Rate Update For Calendar Year 2009*, FR Vol. 73, No. 213.

Medicare Program. *Home Health Prospective System Rate Update For Calendar Year 2010*, FR Vol. 74, No. 216.

Medicare Program. *Home Health Prospective System Rate Update For Calendar Year 2011*, FR Vol. 75, No. 221.

Medicare Programs. *Home Health Prospective Payment System Rate Update for CY 2012*, FR Vol. 76, No. 214.

Medicare Program. *Home Health Prospective Payment System Rate Update for Calendar Year 2013*. FR Vol. 77, No. 217.

Medicare and Medicaid Programs. *Home Health Prospective Payment System Rate Update for CY 2014*, FR Vol. 78. No. 231.

Medicare and Medicaid Programs. *Home Health Prospective Payment System Rate Update for CY 2015*, FR Vol. 79. No. 215.

Medicare and Medicaid Programs. *CY 2016 Home Health Prospective Payment System Rate Update*, 80 FR 39839.

Medicare and Medicaid Programs. CY 2017 *Home Health Prospective Payment System Rate Update*, FR Vol. 81. No. 213.

Medicare and Medicaid Programs. CY 2018 *Home Health Prospective Payment System Rate Update*, FR Vol. 82. No. 214.

Medicare and Medicaid Programs. CY 2019 *Home Health Prospective Payment System Rate Update*, FR Vol. 83. No. 134.

Medicare and Medicaid Programs. CY 2020 *Home Health Prospective Payment System Rate Update*, FR Vol. 84. No. 217.

Medicare and Medicaid Programs. CY 2021 *Home Health Prospective Payment System Rate Update*, FR Vol. 85. No. 214.