Prevention and Resolution for Identity Theft: Practical Advice for Individuals, Business Owners, and Tax Professionals

V. Brooks Poole, Mississippi College, MS, USA
Sheree Corkern, Mississippi College, MS, USA
Hannah Hoffman, Mississippi College, MS, USA

ABSTRACT

Identity theft has become widespread and is rapidly increasing. The Bureau of Justice estimates that 7 percent of U. S. residents over the age of 16 were victims in 2014, and direct financial losses were reported by two-thirds of these victims. Virtually anyone is susceptible and should take measures to ensure their data such as social security numbers, personal information, credit and debit cards, and passwords are protected. Often, financial and emotional distress occurs when confronted with identity theft. Educating students on the seriousness and pervasiveness of this crime is essential. Such information would be valuable for all students and particularly those planning to work in an accounting firm or financial institution. After all, tax preparers attempting to file a tax return may be the first to discover that a client's identity has been compromised. This article reviews prevention, warning signs, and resolution should identity theft occur. Business related course instructors should find this information to be an extremely useful resource to share with their students.

Keywords: identity theft, security, business education

INTRODUCTION

In the current internet era, an individual can access almost every account he owns from anywhere at any time. Cell phone data enables him to survey his checking account before going out to lunch. Free Wi-Fi allows him to pay his power bill at a coffee shop. While on his company's secure server, he may order a new brief case by submitting his credit card information on a web form. In addition to the many times people enter personal information via the web, they also swipe credit cards multiple times a day at gas stations, restaurants, and grocery stores. Not only are individuals' funds susceptible to theft, but their identities are as well.

Identity thieves are involved in a wide variety of fraudulent activities. The United States Bureau of Justice Statistics (2015) defines identity theft as one of three events: (1) unauthorized use or attempted use of an existing account, (2) unauthorized use or attempted use of personal information to open a new account, and (3) use of personal information for fraud. The Bureau's National Crime Victimization Survey found the most prevalent form of identity theft to be the use of another's credit card or bank account information. Often, individuals fail to notice the theft has occurred. Nearly half of the victims from the survey discovered the fraud when their financial institution contacted them about the suspicious activity. About 75 percent experienced financial loss, and those who had new accounts opened in their name faced the largest expenses. Not only can identity theft be financially costly, but it can also take a toll on emotional health, as ten percent of the victims reported the incident to be severely distressing (Bureau of Justice Statistics, 2015).

Unfortunately, the occurrence of identity theft is rapidly increasing. The Bureau of Justice Statistics estimates that 17.6 million, or seven percent, of Americans were victims of identity theft in 2014. In comparison, the Equifax data breach announced in September of 2017 affected about 143 million U.S. citizens, or an astounding 51 percent of the nation's adults. The effects of the breach are expected to spread, even for those who were not immediately affected.

Just as individuals continue to be targeted by identity thieves, identity theft in the business sector is also on the rise. Evidence suggests widespread occurrences of business identity theft, which makes it essential that business students be educated to identify, assess, and manage such risk. The time and effort taken to address just one occurrence can be costly for a businesses' bottom line. Many businesses are at risk of falling prey to this type of crime. Businesses that use credit or debit cards, access online banking, or provide confidential business details stored somewhere such as their attorney's office, may be targeted. All business educators should be advocating the

inclusion of identity theft awareness and prevention in their courses. In today's growing and changing world, business education must address the harsh realities of identity theft and cyber threats, and develop programs to educate its' students in prevention and management. Knowledge and understanding of these potential threats will help prepare students to prevent or recover from such crimes. Ultimately, the goal is to ensure that as future business leaders, students are provided the tools necessary to identify, assess, and manage the risk of identity theft; and in doing so, limit the severity and potential for occurrence.

LITERATURE REVIEW

Several experiments have been performed to discover if involvement in certain activities predicts the likelihood of having one's identity stolen. Reyns and Henson (2016) conducted a study in hopes of finding correlations between routine online activities and identity theft. Based on a random sample of households in Canada, the survey asked questions similar to those asked in the American National Crime Victimization Survey by the Bureau of Justice Statistics. Four online activities were closely examined, including banking, booking reservations, buying goods or services, and social networking. To confirm previous research, the study used linear regression to determine that two of the four activities, online banking and online purchasing, had a high correlation with identity theft (Reyns & Henson, 2016).

Additionally, the University of Texas at Austin Center for Identity has developed a risk assessment model that predicts the occurrence of fraud. The Identity Threat Assessment and Prediction model is a database that collects information from news stories and other sources. It applies analytics to compare threats, trends, and losses. Research finds that the impact of identity theft is usually local with over 99 percent of cases limited to a local geographic area or a particular type of victim. Nearly 34 percent of compromised personal information incidents involve co-workers or family members of victims. Research also finds that emotional distress often has a larger effect on people than financial loss (Harman, 2017).

Often, technological advances come with the negative side effect of creating more ways for criminals to hack into private information. Facial recognition is becoming a more widely used form of identification. The release of the new iPhone X, which uses Face ID, is making people more aware of the potential issues. Robertson, Kramer, & Burton (2017) performed a study to examine the likelihood of devices accepting fraudulent images for facial recognition verification. One experiment tested a mobile device while using photo identification that had been altered by software that combines, or morphs, two different faces. Experimenters pre-loaded a cell phone with either an actual photo of the participant, an "imposter" photo, or a morphed image of the two as the face-match for ID. Then participants tried several attempts to unlock the device with facial recognition. While the phones never gave access when the "imposter" image was uploaded, they did detect the morphed photos as a match to the phone user 27 percent of the time. In another experiment, the researchers asked participants, who were unaware of the purpose of the study, to identify whether two facial images were of the same individual. Some of the photos matched, some were a mismatch, and some of the mismatches had been morphed. Participants accepted 68 percent of the morphed images as matches, leading to a conclusion that identity thieves can use technology to alter images and pass as someone else with fraudulent photo identification. In a second round, the participants were warned that some of the images might be altered, and the "match" response decreased to 21 percent for the morphed images. (Robertson et al., 2017).

Identity theft is not only faced by individuals, but by small businesses as well. In 2016, businesses reported 82,000 cyber incidents, but the total could be close to 250,000 if all cases were reported (Too Small to Fall Victim, 2017). According to the FBI, personal and corporate identity theft are the fastest growing crimes in the nation. Corporate identity theft is a threat to businesses of all sizes. It can occur when others pose as the business to acquire credit, when employees' or customers' personal information is compromised, or when company records are accessed by an outside party. The attack can come from an outsider posing as an employee or from an insider with malicious intent, such as an upset employee or a spy for a rival firm. Recent victims include The Home Depot, Target, and Sony (McGee & Byington, 2015). Businesses often become victims when an employee clicks on a link in a phishing email. Phishing occurs when scammers use fake email addresses or websites to lure individuals into providing personal information. The scammer then uses that data for fraudulent purposes (Schreiber, 2017). Hackers may sell the company's stolen information, use it to harm the reputation of the business, hold it for ransom, or use it for personal gain. Consequently, the company may face issues receiving bank loans, keeping loyal customers, and protecting personal employee data once they have been hacked (Too Small to Fall Victim, 2017).

Contributing to business risk, the rocky state of the economy in 2008 forced many operations to go out of business. When owners discontinue monitoring business accounts and registration information, it invites criminals to use their company name for personal gain. Hackers may take out new credit or steal goods from suppliers. They may file fraudulent reports with the Secretary of State offices or change online business records. If a filing meets the essential requirements, the state offices have little basis to question or reject the documents (Mota, 2016).

Each year the IRS releases a list of the top twelve, or "Dirty Dozen", tax scams for the filing season. In 2017, the number one scam was phishing. Phishing schemes target payroll and human resources services, taxpayers and their CPAs, and government agencies (Schreiber, 2017). In an annual threat report by Cloudmark, 84 percent of the 300 U.S. and UK companies that were surveyed disclosed that phishing attempts had made it through their security defenses (Hernandez, 2016). Next on the Dirty Dozen list was phone scams. Criminals pose as IRS agents and call taxpayers threatening arrest, license revocation, and even deportation. The IRS will contact individuals by mail and will never threaten such things. The third scam was identity theft. The Security Summit Partners, which consists of the IRS, tax practitioners, and state tax agencies, are continuing efforts to safeguard against this criminal act (Schreiber, 2017).

Some of the ideas issued from the 2015 Security Summit meeting included pre-refund authentication and refund fraud detection, using post-filing analytics to prevent fraud, use of a tax refund fraud information sharing and assessment center, identity proofing, and taxpayer education (Demshock, 2016).

DISCUSSION

Risks factors for individuals

An individual's likelihood of becoming a victim of identity theft increases by 12 percent when active in online banking and by 17 percent when buying goods online. Those who have been hacked or been the recipient of phishing emails are dramatically more likely to have their identity stolen. Not surprisingly, those who have personal information posted publicly online are more than three times as likely to fall victim (Reyns & Henson, 2016). Currently, four elements known as "knowledge-based factors," including name, birth date, address, and Social Security number, are being challenged as the best personal identifiers for services (Lemos, 2016, p. 1). Three of the four factors are readily available on a piece of mail or someone's social media account. Experts say that stricter security factors must implemented (Lemos, 2017). Ultimately, everyone who participates in modern society is at risk, so the focus should be on prevention and protection.

Prevention for individuals

Social Security card:

A stolen Social Security number is possibly the worst form of identity theft. Individuals should always ask why the number is needed before readily providing it to doctors' offices or companies. An alternative form of identification may be acceptable. A Social Security card should never be regularly carried in a wallet (Gerstner, 2015). Proper and secure locations for storage include safe deposit boxes, safes, and lock boxes. Parents should also be cautious when school forms require their child's Social and never hesitate to ask why it is necessary (Gerstner, 2013). When emailing sensitive information, such as a tax form with a Social Security number, individuals should save the document as a PDF and encrypt the attachment rather than typing directly into an unprotected email (Weber & Horn, 2017). Furthermore, a stolen Social Security number and a matching name are the only two vital pieces of information that a criminal must have to file someone else's tax return. A refund will likely still be issued if the rest of the information, although fictitious, appears to be legitimate.

Personal information:

Individuals should use much discretion when posting personal information to online profiles. Phone numbers and birthdates should not be shared on social media sites. Children are also a target, so parents should be aware of what their kids are sharing about themselves. Receiving suspicious mail addressed to a child is a sign that someone has accessed his or her personal information (Gerstner, 2013). During the wake of phone scams throughout the nation, the IRS issued a statement in May of 2016 verifying that they would never contact an individual via phone call. Therefore, taxpayers should never reveal any personal information to anyone who calls claiming to be the IRS (Kess, Grimaldi, & Revels, 2017). Additionally, individuals can protect their information by opting to use the

personal hotspot feature on their smartphone or device rather than the free Wi-Fi offered in airports and coffee shops. Hard drives should be encrypted when possible. Individuals should have at least two data backup systems to protect photos, videos, and important documents (Weber & Horn, 2017).

Passwords:
To prevent fraudulent access to personal accounts, users should provide a different password for each site, especially for banking sites. Serious financial loss can result if a criminal discovers that the same login combination unlocks an individual's checking, savings, and credit card accounts. Passwords should be long and contain a combination of uppercase, lowercase, symbols, and numbers (Gerstner, 2013). Login information should never contain the word "password," and username and passcode should never be identical. A personal identification storage system is a helpful aid in remembering numerous complicated phrases. Password vaults, such as Dashlane or 1Password, use a single passphrase to create and securely store complex passwords that can be accessed from desktop, laptop, or handheld device. Changing login information every three to six months is a good practice for highly sensitive accounts such as banking and investments. Home internet users should use a sophisticated Wi-Fi passcode because the signal often reaches neighbors or nearby parks and shops. A guest network with a separate password allows visitors to use the home internet, but the safeguard will not permit them to access personal files and devices (Weber & Horn, 2017).

***Credit cards*:**
Preventative measures to thwart against identity theft include zero-liability policies that offer full refunds for any amount used for fraudulent purchases. Most major credit card companies follow this standard if the fraud is reported in a timely manner. Additionally, there is second-factor authentication, which alerts users when unauthorized access is attempted on their account (Kess et al., 2017). Individuals should frequently watch their checking and credit card accounts for fraudulent transactions and set up alerts for purchases over a certain dollar limit, such as $150 (Gerstner, 2013). Some credit card companies have a feature that will send an email alert if the card is charged when not physically present, such as with online purchases. People should avoid allowing devices to store credit card information, especially on shared or public computers. It is a good practice to keep receipts until transactions have cleared or until a monthly statement is issued. An individual can match receipts to verify that every purchase made was a legitimate one. Matching receipts is also a way to ensure that the correct amount was charged, especially after a meal out when the wait staff adds the tip after the customer has left.

RESOLUTION FOR INDIVIDUALS

The Federal Trade Commission (2017) maintains a website to guide those who have fallen victim to identity theft. There are three immediate steps to take upon discovering the theft. First, the affected individual should call the companies where it is certain that fraud has occurred and ask them to close or freeze the account. Then logins and passwords should be changed. Next, the victim should call one of the three credit bureaus, place a free 90-day fraud alert and get a free credit report. The third step is to report the theft to the Federal Trade Commission by completing the online form or calling the department. Some people may choose to file a report with the local police department as well. After completing the three urgent steps, the individual should begin closing any new accounts that were fraudulently opened, calling businesses to get the charges removed, writing a letter to each credit bureau to correct the affected credit report, and possibly getting an extended fraud alert or credit freeze. Depending on the severity of the situation, a victim may need to replace government-issued identification and clear his or her name from criminal charges. The FTC website provides detailed guidance for each of these steps (Federal Trade Commission, 2017).

Comparatively, the Internal Revenue Service provides guidance for individuals who, when filing their own tax return, discover their identity has been stolen. When an e-file return is rejected, the taxpayer should file the tax return by paper and complete Form 14039, Identity Theft Affidavit. The form goes to the Identity Theft Victim Assistance organization and usually takes 120-180 days to resolve. Certain victims will receive an Identity Protection Personal Identification Number (IP PIN) in a CP01A letter from the IRS. The IP PIN will be used the next filing season to help protect the individual's identity. Some taxpayers will receive a new IP PIN annually to enter on the tax return for identity verification. If the IRS Taxpayer Protection Program suspects that a fraudulent return has been filed under the taxpayer's name and Social Security number, they will send a notice requesting identity verification within 30 days. When an individual is identified as a victim, the IRS marks the taxpayer's account with an indicator to help protect the individual in the future (IRS Updates, 2016).

If an individual suspects that he has fallen victim to credit card fraud, he should contact one of the three major credit bureaus, Equifax, Experian, or TransUnion, which will alert the other two. If a person discovers a false account has been opened in his name, he should notify the company and place a fraud alert or credit freeze. An initial fraud alert is free, lasts 90 days, and requires companies to take extra care in identity verification before issuing credit. An extended fraud alert lasts seven years. A credit freeze usually requires a small fee and blocks new creditors from accessing an individual's credit report. This method is simple security if an individual does not take out new credit frequently, and the freeze can be lifted with an additional fee (Gerstner, 2015).

CONSIDERATIONS FOR BUSINESS OWNERS

Small and medium-sized organizations with good credit ratings are targets for corporate identity theft. Many perpetrators pretend to be a customer or supplier and request payment from the business. To protect a company, management should first know their customers. Employees should always check for the padlock symbol in the address bar of any customer's or supplier's website. They should also check the company registration number, validate delivery addresses, run a domain name check, and get a free company credit check. Upper management should create an atmosphere of awareness and openness when suspicious activity takes place (Mota, 2016). To further protect the company, management should also develop a corporate prevention plan, protect company documents, monitor credit reports, and avoid using master usernames and passwords (McGee & Byington, 2015).

One of the most common ways for businesses and individuals to fall victim to identity theft is through phishing emails that appear to come from trusted sources. Just one compromised identity in a company can give a hacker entry into an entire organization. IBM recommends that companies educate employees to be aware of phishing attempts and implement controls to deter hackers. Peer-phishing attacks occur when hackers impersonate upper management. Emails appear to come from within the organization, and colleagues are likely to respond to the requests of bosses. Microsoft's Azure Active Directory Identity Protection is an add-on to Microsoft's cloud-based identity software. The program catches uninvited users on company networks and blocks their access. If suspicious activity is detected, the program can block a user, require a user to answer further identification questions, or require a user to change their credentials (Hernandez, 2016).

Even national policies exist to protect companies and consumers. The Red Flag Rule was created in 2011 by the Federal Trade Commission, federal bank regulatory agencies, and the National Credit Union Administration. The policy mandates that companies have plans in place to mitigate activities, or "red flags", that would cause or reveal the presence of identity theft. All organizations subject to the Fair and Accurate Credit Transactions Act of 2003 must create a written plan for identity theft prevention and detection. Four categories of warning signs must be identified in the program. Category one includes alerts from a consumer reporting agency, such as a credit freeze, a large number of new credit issuances, or a closed account due to misuse. Category two warning signs are suspicious documents. Such documents may be identification that appears to be counterfeit or reassembled after destruction and presentation of photo ID that does not appear to be legitimate. Category three involves personal information, such as a Social Security number that has not been issued or an inconsistent address and phone number. Category four signs cover strange account activity, such as the request for new credit lines soon after a change in address, a major change in spending patterns, and sudden purchases on an account that has been inactive (Kunick & Posner, 2011). With these policies in place, a business can catch fraud before it happens, or it can reduce the consequences by acting quickly when fraud does occur.

CONSIDERATIONS FOR TAX PROFESSIONALS

In yearly reports from 2009 to 2014 the Federal Trade Commission stated that tax-related identity theft was the most prevalent form of identity theft. This type of fraud occurs when a scammer uses someone else's Social Security number to file a tax return before the victim and receive a refund. In 2012, the Internal Revenue Service anticipated a $21 billion loss over a five-year span (Demshock, 2016). According to *The Tax Adviser* and the *Journal of Accountancy* annual survey, nearly 60 percent of the practicing CPAs who responded had clients affected by identity theft during the 2016 tax season. From 2015 to 2016 there was a 15 percent decrease in the number of individuals who knew they were affected before attempting to file their returns. Preparers or victims are typically unaware of the theft until they attempt to file and the return is denied because the victim's Social Security number has already been

used on a fraudulent return (Bonner, 2017). Upon discovering the theft, CPAs are put in a position where sometimes unused relational skills must be exercised in communicating the bad news and the next steps to an unknowing client. Although the IRS has implemented tax return screening programs and limited the number of refund deposits allowed for a single bank account, the Treasury Inspector General for Tax Administration admits that the battle to stop tax identity fraud persists (Bonner, 2017).

Warning signs for client identity theft include the following (Dishman, 2017):

- IRS reject code R0000-902-01 indicating the client's Social Security number was already filed in a return for the year
- A report stating that a client has a balance due, collection action, or refund offset for a year in which they did not file
- IRS records stating the client claimed wages from an unknown employer
- A business client receiving a notice about an amended return or fake employees
- Evidence of physical alterations to tax forms such as W-2s and 1099s

Preparers should be aware of these indicators and act quickly when they notice something suspicious. Tax professionals should communicate the warning signs to their clients and request to be notified immediately if any of these things occur throughout the year.

The AICPA issued a statement to the IRS Oversight Board listing tips that tax advisors can perform to protect their clients (Demshock, 2016):

- Lock desk and filing cabinet drawers
- Use encrypted external drives
- Blur or truncate Social Security numbers
- Install antivirus
- Use password-protected emails

Taxpayers can help prevent identity theft by filing returns early in the season, shredding important documents, and checking credit reports regularly.

Identity thieves who file fraudulent tax returns not only steal refund money from the government and the victims, but they also negatively affect the employers for whom they claim to work. If the tax return is not flagged as fraudulent, the IRS will attempt to collect the payroll taxes from the company reported on the fake W-2. Then it becomes the employer's responsibility to prove to the IRS that those wages were never paid. Employer Identification Numbers (EINs) are on every W-2 from the company and are often available on the web. While a Social Security number can only be used to file one fraudulent return, a stolen EIN can be used multiple times. Complicating matters is the fact that W-2s are filed with the Social Security Administration rather than the IRS. To prevent EIN theft from occurring, there is a program available that allows some large employers to send drafts of their W-2s to the IRS before they are mailed out to employees. The IRS will match W-2 information against refund claims. Employers should reconcile tax payments to the payroll system, monitor IRS notices, and never pay unwarranted tax deficiencies without ensuring that fraud is not in play (Salam & Sypker, 2013).

CONCLUSION

Ultimately, every individual, business owner, and tax professional should be aware of the risks and consequences of identity theft. Dealing with identity theft is often financially and emotionally distressing, time consuming, and a major inconvenience. Because virtually everyone is vulnerable to attack with data so easily accessible on the web, individuals should show prudence in providing information over the phone or on social media. Social Security cards should be kept secure, and the numbers should not be shared unless absolutely necessary. Individuals should also treat credit and debit card information with special care and check online accounts often in order to locate any fraudulent purchases. Passwords should be complicated and varied for each account. The Federal Trade Commission and the Internal Revenue Service both provide guidance for those who discover their personal information has been compromised. Small businesses are not excluded from the risk and may experience two types of identity theft. First, sensitive information about individual employees or customers may be exploited through hackers or disloyal workers. Secondly, others may fraudulently do business under their trade name. Management should have information security and fraud prevention plans in place to deter the theft of sensitive information. Lastly, tax

preparers deal with client identity theft when preparing tax returns. As professionals and advisors, they have the burden of educating themselves and their clients about the risks and solutions associated with identity theft. There are warning signs and prevention steps that both preparers and clients should follow.

REFERENCES

Bonner, P. (2017). CPAs contend with tax ID theft. *Tax Adviser*, *48*(4), 10-12.

Bureau of Justice Statistics. (2015). Victims of identity theft, 2014. 1.

Demshock, H. M. (2016). What can be done to combat tax-related identity theft? *Journal of Financial Service Professionals*, *70*(3), 16-19.

Dishman, S. (2017). Preventing tax-related ID theft. *Accounting Today*, *31*(1), 6.

Federal Trade Commission. (2017). Theft recovery steps. 1.

Gerstner, L. (2013). What you need to know about identity theft. *Kiplinger's Personal Finance*, *67*(6), 70.

Gerstner, L. (2015). How to fend off ID thieves. *Kiplinger's Personal Finance*, *69*(9), 32-39.

Harman, P. L. (2017). Assessing identity theft risks. *Claims*, *65*(5), 12-14.

Hernandez, P. (2016). Microsoft Azure AD service keeps an eye on suspicious behavior. *Eweek*, 8.

IRS updates identity theft victim assistance information. (2016). *Federal Tax Course Letter*, *30*(3), 14.

Kess, S., Grimaldi, J. R., & Revels, J. J. (2017). Identity theft: Tax and financial considerations. *CPA Journal*, *87*(1), 66-68.

Kunick, J. M., & Posner, N. B. (2011). Following the red flag rules to detect and prevent identity theft. *Information Management Journal*, *45*(3), 25-28.

Lemos, R. (2017). Identity verification becomes trickier in wake of Equifax breach. *Eweek*, 2.

McGee, J., & Byington, J. (2015). Corporate identity theft: A growing risk. *Journal of Corporate Accounting & Finance (Wiley)*, *26*(5), 37-40.

Mota, D. (2016). Stolen identities. *Business Credit*, *118*(4), 34-36.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy & Comparative Criminology*, *60*(10), 1119-1139.

Robertson, D. J., Kramer, R. S., & Burton, A. M. (2017). Fraudulent ID using face morphs: Experiments on human and automatic recognition. *Plos ONE*, *12*(3), 1-12.

Salam, D., & Sypker, D. (2013). Tax refund scams can involve costly employer identity theft. *Journal of Tax Practice & Procedure*, *15*(2), 31-55.

Schreiber, S. P. (2017). 2017's dirty dozen tax scams. *Tax Adviser*, *48*(5), 6-7.

Too small to fall victim to identity theft? Think again. (2017). *Inc*, *39*(3), 44.

Weber, R. M., & Horn, B. D. (2017). Breaking bad security vulnerabilities. *Journal of Financial Service Professionals*, *71*(1), 50-54.

V. Brooks Poole, CPA, CIA, MTAX, is an instructor of financial accounting and taxation at Mississippi College in Clinton, MS. His research focus is practitioner-geared topics in taxation and international financial accounting. Specific areas of research interest include estate taxation and planning, federal and state income tax planning, international convergence, ethics in financial accounting, and equity and social justice in higher education.

Sheree Corkern, CPA, Ph.D., is an assistant professor of financial accounting at Mississippi College in Clinton, MS. Her area of research is pedagogy and applied research in financial accounting.

Hannah Hoffman earned her Bachelor of Science in Business Administration with a major in Accounting as well as her Masters in Accounting from Mississippi College. Her area of research is ethics and trends in the accounting profession.