Spring 5-20-2019

Understanding the Value of Mitigating Fraud Risk for Small Businesses with Cash Management

Vivian Denkins
La Salle University, danielsv1@student.lasalle.edu

Understanding the Value of Mitigating Fraud Risk for Small Businesses with Cash Management

Vivian G. Denkins

La Salle University

Author Note

Vivian G. Denkins, Department of Cybersecurity, La Salle University

Vivian G. Denkins, Wyncote, PA 19095

Contact: danielsv1@student.lasalle.edu

Understanding the Value of Mitigating Fraud Risk for Small Businesses with Cash Management

Table of Contents

Abstract

Most companies are interested in increasing their revenue, growing their customer base, and maintaining their business for as long as the market will allow. While some businesses are looking to last beyond the average life cycle of 10 years (U.S. Small Business Office of Advocacy, 2018), most do not consider fraud as a major impact that could end their business. Fraud does exist, even for the small business owners. However, most owners decide to take their chances against fraudulent schemes and carefully guard their business using their own measures. According to the Association for Financial Professionals (AFP) (2019), the 2018 AFP Payments Fraud and Control Survey states that 82% of finance professionals report that their companies were victims of payment fraud. Businesses encounter fraud and can lose thousands of dollars as a result of it. Some of the common types of fraud a small business may encounter are payroll, invoice, wire, and online payment threats, such as phishing (Anderson, Durbin, & Salinger, 2008). All of these are common ways small businesses are attacked. As companies make purchases, they must realize that any payment type is susceptible to fraud. Consider counterfeit bills, forged checks, and unauthorized cardholder use, these are all fraud related concerns (Anderson et al., 2008). These incidents can prove costly and possibly result in revenue losses.

A business operating cycle consists of purchasing materials, converting those materials into goods and services for customers to buy, collecting the funds from sales of the goods or services, and then, the cycle continues (Masson, 2001). Financial institutions help businesses manage their operating cycle more effectively by providing solutions that improve the cashflow. Banks use cash management services to address the cashflow needs, including measures that will help mitigate potential fraud. With protocols in place, a business can detect fraud and prevent it. However, some owners refuse to use fraud mitigation products. Owners resolve that banks should protect their accounts anyway, even when it comes to Internet fraud. In addition, the cost and time simply does not justify having full protection (Moore, 2018). This behavior could lead to company losses and the end of their business.

Keywords: fraud, small business, cash management, ACH, positive pay

Understanding the Value of Mitigating Fraud Risk for Small Businesses with Cash Management

Introduction

The U.S. Small Business Administration Office of Advocacy (2018) defines a small business as an independent establishment with fewer than 500 employees with revenue of $7 million or less. In 2015, there were more than 30 million small businesses which comprised 99.9% of all industries (Office of Advocacy, 2018). This is a major part of the United States economy. From 2005 to 2017, nearly 80% of small businesses survived within their first year of establishment (Office of Advocacy, 2018). One of the causes of small business failures is poor management of the company's financial resources (J. W. Carland, J. C. Carland, & J. W. Carland, 2001). Hunter's (2011) study proposed that failed businesses did not have a long-term strategy, they tend to react to situations as they arose (Hunter, 2011). The primary objective of a business is to maximize shareholder value. Businesses should develop practices and techniques essential to protecting and managing their cash to ensure longevity.

Cash is the integral part of a company's overall operations (Masson, 2001). Managing cash is required to sustain the company. The business will find it hard to survive without cash or liquidity (Sharma, 2008). For example, a business cycle occurs when the company purchases materials, converts those materials into goods and services for their customers to buy, then collects the funds from sales of the goods or services, and ultimately, uses the cash to purchase more materials to continue the cycle (Masson, 2001). Cash is collected from sales generated and it is needed to fund the business. Managing the flow of funds within the operating cycle is called cash management (Masson, 2001). Cash management encompasses all payment methods, which includes checks, wires, ACH debit and credit items, business-to-business payments (B2B),

business-to-consumer payments (B2C), mobile payments, and credit cards. While attention is on the day to day functions surrounding the operating cycle, some managers may disregard or overlook the need to monitor risk (Carland et al., 2001). Small businesses are at a greater risk of fraud because they have less anti-fraud controls in place (Moore, 2018). This paper will focus on business financial risk associated with fraudulent activity and some of the measures to help mitigate fraud.

Banks are needed to provide relationship financial services to help businesses function (Masson, 2001). If the company needs a loan for the purpose of capital investments, or to purchase items such as equipment, or even to fund a project, they seek out a bank to meet those specific needs. A bank is also available to help the business carry out daily activities, such as check writing, depositing, disbursing, investing money, and utilizing solutions to help their cashflow. Banks provide businesses with a relationship team that consist of a banker partnered with a cash manager (Masson 2001). Both roles build trust by understanding the business and provide solutions for the company to function more efficiently (Masson, 2001). Banking solutions are designed to integrate well with the business operating cycle (Masson, 2001). Sharma's 2008 study confirms that companies use banks to help with the "transfer and payment of funds, collection and concentration of funds, sweep (investment) account services, and information reporting" (p. 79). Banks help the business by "accelerating the receipts and slowing down the disbursements" with appropriate cash management products (Sharma, 2008, p. 79). In lieu of today's robust payment environment, businesses are interested in more convenient ways of getting money from their customers. Financial institutions find themselves partnering with Fintech companies to offer digital solutions (Son & Kim, 2018). Fintech companies are payment systems that are a combination of financial and information technology services (Son &

Kim, 2018). Therefore, the specialized role of a cash manager is vital when providing solutions to help manage the company finances, and in mitigating all types of financial fraud.

When fraudulent activity occurs within a business, it is sometimes difficult to discover what really happened. Organizational and internal fraud can go undetected for months or maybe years before they are identified. There are usually no internal controls in place, audits or external reviews (Carland et al., 2001). Therefore, it will take a longer time to determine the cause of the fraud. Either way, fraud mitigations should be in place to protect the company. This paper will define cash management, how it works, and the solutions to help mitigate financial fraud. In addition, this paper will show how fraud solutions can help small businesses stay protected from different types of financial fraud.

According to the Association for Financial Professionals, (2019), the AFP's 2019 Payments Fraud and Control Survey, found that 82 percent of finance professionals reported that their companies (revenue less than $1 billion) were the target of payments fraud in 2018, 70 percent of them were check fraud victims, and 43 percent of organizations had financial loss as a result of payments fraud. This high percentage is not exclusively for small businesses; altogether, the findings are staggering. Fraud mitigation solutions are not entirely fraud proof, however, education and implementing the right solutions can help decrease the number of incidents dramatically. Based on the 2018 Report to the Nation (ACFE, 2018), small businesses lost twice as much per scheme to fraud. The median loss was $104,000 with 100 plus employees and $200,000 median loss for less than 100 employees (ACFE, 2018). Occupational or internal fraud seemed to be the most prevalent of cases involving company losses (ACFE, 2018). Small businesses have a lot more to lose when there is an unsuspecting loss or one that is difficult to track. The impact can be detrimental to the company and may be difficult to recover. For

example, a woman working as the entire accounting department for a lighting store stole $416,000 over eight years (Kramer, 2013). She wrote checks made payable to herself, deposited them in her personal account, and indicated in the company register that the check was voided (Kramer, 2013). She would then overstate the amount in the next checks she wrote to vendors. There were no annual reviews of the records or inventory count (Kramer, 2013). "The store was nearly bankrupted as a result of her scheme" (Kramer, 2013, p. 15).

According to Hess and Cottrell (2016), "companies can lose 5 percent of their revenues to fraud every year and fraud is a significant contributing factor to small business failure" (p. 13). Fraud in a small business affects the employee productivity and morale (Hess & Cottrell, 2015). When management sets the appropriate tone about fraud, the company benefits from a supportive environment. This type of setting discourages organizational and internal fraud.

What is cash management

Research by Prasad Das and Parida (2016) states that "cash management means the management of liquidity to meet day to day activities" (p. 102). The method of reducing days in account receivables and increasing the days on payables will help the business avoid insolvency (Prasad Das & Parida, 2016). This means that when money comes in slowly the business has difficulty operating. They may have to borrow money, liquidate assets, or reduce production. Therefore, using cash to meet some of the unpredictable or unplanned events is common and should be a precautionary motive for the company (Prasad Das & Parida, 2016). Cash or some form of payment method (checks, credit card, electronic payment) is needed to meet the daily requirements of the business (Masson, 2001).

Hines, Hurtt, & Langsam, (2000), credits Vanderbilt University professor of management, Germain Boer, for creating the term, “cash gap” as the “imbalance between cash inflows and cash outflows” (p. 16). Cash management manages the cash inflows and outflows of the business. If the inflow and outflows matched daily, there would be no need for cash management, but rarely does this happen. There are times when the disbursements will exceed receivables, and conversely, receivables will exceed the disbursements (Prasad Das & Parida, 2016). However, as Masson (2001) mentions, the business operating cycle should continue. Cash management structuring helps businesses find options to lessen the stress while waiting for receivables and meeting their payment obligations (Prasad Das & Parida, 2016).

Also, Hines et al., (2000) supports that “cash management is defined in terms of short-term assets and liabilities to include collection of accounts receivable, payment of accounts payable, and concentration of cash balances in order to maximize interest earnings” (p. 15). Both definitions of cash management show that controlling the cash flow makes it challenging to predict and yet unique to each business. For example, a retail store must collect cash before the person leaves the store, conversely, a manufacturing company may send their payments over a 30-day payment period (Hines et al., 2000). However, monitoring the receivables and keeping in contact with customers can decrease the average receivables period or less of a ‘cash gap’ (Hines et al., 2000).

Banks understand the business operating cycle and the need for owners to manage their cash. The use of cash management solutions helps businesses effectively streamline their daily cashflow by providing them with tools to make decision based on the company needs and concerns (Hines et al., 2000). Reviewing some of the basic solutions will depict how cash management works for most businesses.

How cash management works

Cash management provides systems and processes that speed up collections, delay the disbursement of cash, and allow for information to help make decision about the business funds (Masson, 2001). Some collection and disbursement solutions use the same methods including, checks, automatic clearinghouse (ACH), digital payments and receipts, wire capabilities, or credit cards (Masson, 2001; Holbrook, 2017). Each tool helps the company accomplish their daily tasks. The decision to use the appropriate solution is based on the needs and structure of the company and its customers.

Hines et al. (2000), conducted an interview with Phoenix-Hecht, the leading nonbank cash management consulting company, and found that there are more than 1,500 different types of cash management services offered to companies. Some products are basic, and some are highly complex based on the needs and systems of the company (Hines et al., 2000). Digital payments have been on the rise since the 90's with technology-enabled tools that support websites, shopping carts, and global order fulfillment (Holbrook, 2017). Any size business can compete on the global scale with well-established networks (Holbrook, 2017). For the purpose of this paper, some of the basic types of cash management services that directly engage fraud mitigation are information reporting, check reconciliation, ACH with online payments, and wires services (Hines et al., 2000).

Information reporting gives a company access to view the business accounts, conduct account transfers between accounts, make stop payments on checks, initiate wires, and carry out other movement of funds (Masson, 2001). Today, many account owners can view their activity on their mobile phone through the bank's online banking app. Access to detail activity can shed

light on the company's cashflow quickly. It is important that authorized users are given the proper roles and functions to carry out their tasks with a need to know basis (Masson, 2001). Most information reporting tools are built where a system administrator can grant access to other users within the company (Nonprofit World, 2018). There are multi-factor authentication phone apps to download which are accessible for viewing and requiring money to move in or out of the account (Tommasi, Catalano, Fornaro, & Taurino, 2019). Also, there are levels of approval required to initiate or approve funds or to change any vendors lists of which the company is associated (Nonprofit World, 2018).

Having the appropriate persons access accounts may seem like common tasks but many business managers get relaxed about this process. If not careful, the wrong users could have access to all accounts and could potentially compromise the business, especially while no one else is auditing their behavior online (Hess & Cottrell, 2015). Consider the small medical clinic with an estimated loss of $757,000 because they did not review their accounts daily (Kramer, 2013). The owner hired a new manager that never took vacation time nor called in sick, she was always there to receive the deposits, statements, and any other funds related to the business (Kramer, 2013). She was found guilty of skimming deposits from the business (Kramer, 2013). The owner should have regularly checked his mobile phone for account activity information to verify against the total receipts (Kramer, 2013).

The number of breaches exposing online IDs rose from 22 in 2009, to 342 in 2013 (Sullivan, 2014). Dual control approvals can help minimize certain fraud risks (Masson, 2001). Small businesses find themselves trusting their employees but, it is also good to verify everyone involved with the finances. People make bad decisions sometimes, so it is beneficial to be mindful of behaviors that stand out from the norm (Moore, 2018).

Checks reconciliation works with a demand deposit account where a company can write checks to pay for goods and services (Hines et al., 2000). The bank helps customers reconcile their accounts by providing a list of checks paid against the company's account (partial reconciliation) or the bank provides a list of issued, paid, and outstanding checks based on the customer's check file (full reconciliation) (Masson, 2001). These two types of reconciliation are important because they provide the status of all checks and it helps to make reconciling effortless.

Company funds should be protected from any unauthorized use by enforcing written policies and internal controls, maintaining check reconcilement, and implementing banking services such as positive pay. These are good measures to have in place (Masson, 2001). Written policies and internal controls include separating functional duties for collection and disbursement of funds (Masson, 2001). Companies should authorize signers to endorse checks with a set maximum dollar amount and use check stock with safe paper and watermarks that are difficult to replicate (Masson, 2001). Storing checks in a safe place or instituting checks safekeeping on CD-ROMs for storage are all good ideas to implement. These internal controls are good to put in place, however, once a check is stolen or reproduced a fraudster will create havoc in a matter of time.

Positive pay service works well with check reconciliation. Through the reconcilement of the accounts, positive pay service matches check serial numbers and dollar amounts against the company's issued checks (Masson, 2001). If there are any items with duplicate check numbers, altered amounts, or out of sequence, the bank will alert the company so they can decide to 'pay or return' the check (Masson, 2001). For example, check 1234 is issued to John Smith for $100. The check is uploaded by the company through the online banking system. When John Smith's

check is presented for payment and the amount is altered to read $1,000, the bank will alert the company via mobile banking that this check is suspicious based on what was entered and uploaded to the bank. An email, text, or banner will alert the company of the altered check. Checks are highly exposed to various types of fraudulent activity (Messmer, 2012). Consider that AFP confirms that most fraudulent techniques used were the creation of counterfeit checks, altering the payee names on checks used by the company, and altering the dollar amount on the checks (AFP, 2016). Positive pay can deter most check fraud situations and it is widely used for this purpose (Masson, 2001).

Positive pay services do not protect against fraudulent endorsements (Masson, 2001). If the check number and dollar amount is correct, then it is possible that the fraudulent endorsement will not be caught. The term 'holder in due course' occurs when a fraudulent check is cashed in good faith (Masson, 2001). For example, in the case of a check cashing company, the company may be liable for this item if the check cashing store took the check in good faith without any defects and believed the check was legitimately negotiable (Masson, 2001). Although checks are not going away, they have declined in volume but not in value (AFP, 2019). Because of this, positive pay mitigation will continue to be offered. However, technology advancements are making electronic payments easier and accessible to all (AFP, 2019) and fraudsters are increasing their attempts to attack all payment methods (AFP, 2019).

Automated Cleaning House (ACH) is another type of cash management service that provides an alternative to check writing (Masson, 2001). ACH is the electronic transfer of funds from one bank account to another. ACH items can either be a receivable or a payable transaction. For example, "vendors may issue ACH debits against customer accounts or customers may issue ACH credits to pay vendor accounts" (Masson, 2001, p. 97). ACH items

can be issued for credit or debit for the same day or future dates (Masson, 2001). The format and timing can be discussed between the parties.

The advantage of using ACH transactions is that companies can reduce the amount of administrative paperwork and the cost of account reconciliation, and increase efficiencies (Hines et al., 2000). ACH transactions are less expensive and safer than checks. Also, the cost of an ACH transaction is considerably less expensive (about 25 to 35 cents per transaction) than the cost of wires (about $12 to $75 per wire) (Hines et al., 2000). The network of ACH payments increased in number 5.7 percent and 6.9 percent by value from 2016 to 2017 (National Automated Clearing House Association [NACHA], 2019). Since ACH transactions have increased, data has become more valuable to fraudsters (Sullivan, 2014). The loss in total payment value of ACH payments resulted in $1.2 billion in the U.S. (Sullivan, 2014). As the use of electronic payments have increased so have the security features. Therefore, small businesses must implement security measures to help mitigate fraud.

ACH transactions are used for payments to vendors, direct deposit of payroll, and collection of funds. As funds can only be transferred between banks, businesses may think that this gives a sense of security and protection. In Messmer's (2012) reference to the AFP's survey of 500 businesses, they "were asked how monetary fraud hit them in 2011" (p.1). They found that 85 percent of the respondents were impacted by fraudulent checks, while 23 percent mentioned ACH debit" (Messmer, 2012, p. 1). Fraudsters will use account information to create counterfeit checks or purchase items online (Messmer, 2012).

It is important for small businesses to increase their methods of receiving payments in order to accommodate most vendors and consumers today. For the benefit of consumers, information technology and finance payment systems, or Fintech businesses, have expanded into

the banking business area of data analysis, financial software, and payment platforms (Son & Kim, 2018). This technology edge will potentially change banks by causing them to work with Fintech companies and lead to lower costs in creating payment platforms (Son & Kim, 2018). The smartphone industry, led by Apple's iPhone, provides users the flexibility to purchase items with their phones (Son & Kim, 2019). Chun (2018) reports that "cybersecurity ventures predicts cybercrime's global cost will reach $6 trillion by 2021", (p. 2). As small businesses partake in a portion of this number it is difficult to determine how much risk or damage it could cause companies and account users (Chun, 2018).

Surprisingly, vendors continue to use checks to pay other companies. AFP (2019) reports that checks are still the most used payment method for business-to-business, and therefore, checks are still common targets for fraudsters. Technology advancements surrounding electronic payment processes are becoming easier to implement. At the same time perpetrators are aided by those same technologies to attack payment methods. Therefore, the "decline in check fraud activity has been offset by the increase in payment fraud" (ACH transactions and wires) (AFP, 2019, p.5).

Wire transfers are another cash management solution for businesses. Wires are more expensive, due to their speed (only minutes), finality of payment (the Federal Reserve guarantees payment), and more importantly, wires are more reliable and secure than checks (Masson, 2001). Wire transfers are received as cash that is available for immediate use. The difference between a wire and an ACH transfer is the cost and the timing (Masson, 2001). Wires do not have a time delay while ACH items occur within the day or can be batched with a group of ACH transactions for future credit or debit (Hines, et al., 2000). Both services have incoming and outgoing transactions.

Business Email Compromise (BEC) adds to the list of elements attackers use to steal company money or sensitive information (AFP, 2016). The attacker gains access to the company email account and mimics the owner's identity to defraud the company. BEC have increased from 64 percent in 2014 to 80 percent in 2018 (AFP, 2019). The typical compromise involves sending a fraudulent invoice to an employee persuading them to send payment (wire) to a bank account different from their normal vendor (AFP, 2016). Companies must be aware and prepared to deter this type of attack.

The cash management solutions mentioned are some of the most basic services that could benefit a small business operating cycle. As previously mentioned, there are over 1,500 types of cash management services offered to companies, each serving a specific purpose (Hines et al., 2000). For example, a more complex service may include the ability to send the customer one file that consists of check images and amounts, credit card payments, ACH, and wire payments. The file may be uploaded to a company's enterprise system for them to update their receivables. This service is called an electronic lockbox (Masson, 2001). The actual checks are mailed to a post office box on behalf of the business, "the bank processes the checks received and deposits the payments directly into the company's account" (Hines et al., 2000, p. 18). The electronic feature elevates the service by allowing the company to 'go green' and not receive any paper items to process. A lockbox service may be an inexpensive assistant compared to the salary of someone doing this job internally. A net benefit analysis can be presented to the business to show the lockbox savings compared to the company's internal processing cost (Masson, 2001).

The fraud deterrent feature means paper checks are not handled, thereby, decreasing the opportunity for losing checks or altering them. There is a minimal opportunity to exploit fraud when the items are converted into electronic files or mailed directly to a post office (Hess &

Cottrell, 2015). These services which include check reconciliation, ACH transactions, and wire transfers, all appear to be more practical cash management solutions for small businesses due to their simplicity.

Solutions to mitigate fraud

Understanding the foundation for effectively controlling the flow of funds starts with basic knowledge. First, the business needs to know their responsibility when it comes to conducting transactions. The bank is ***not*** always the first who is fully responsible for losses. This is highlighted in the Uniform Commercial Code (UCC).

The UCC is not a law but a product of two private entities which includes the National Conference of Commissioners on the Uniform State Laws and the American Law Institute (SBA, 2019). The UCC is recommended for governing state commercial transactions (Masson, 2001). Article 3 of the UCC affirms that "there must be a negotiable instrument for the transaction, in this case, a check, and there is a need to exercise ordinary care to the extent of the check" (Masson, 2001, p. 78). Article 4 recognizes the relationship between the bank and its customer (Masson, 2001). For example, the bank can decide to not pay checks more than six months old (stale date) (Masson, 2001). Additionally, it is the customer's duty to report an unauthorized signature or alteration of their check.

Companies also have an obligation to examine their bank statements for any discrepancies or unauthorized actions within 30 days after the statement was sent (Masson, 2001). It is important that companies view and reconcile their account accurately and timely. If not, the company may be held responsible for the ordinary care related to check issuance (Masson, 2001). The company should also inform the bank of any forgeries in a timely manner

(Masson, 2001). In 'good faith', the company should handle their account with reasonable care (Masson 2001). Disregarding or overlooking potential incidents could jeopardize the company. Actively reviewing accounts regularly could identify any unusual patterns or behaviors. Nearly all banks offer the ability for companies to view their account activity either with their PC, tablet, or mobile app. Information is as accessible as one uses it.

Next, the business should consider making checks less appealing to fraudsters by converting to safer electronic methods. With the increase of electronic payments businesses can position themselves by switching to a less risky environment. Checks have proven that fraudsters are highly attracted to them as they easily create counterfeits with some of the best technology. The AFP (2016) reports that organizations are moving to 100 percent direct deposit of payroll to avoid fraud problems. National Automatic Clearinghouse Association (2019) released that ACH payments increased 6.9 percent by value from 2016 to 2017. Electronic payments have many "advantages over checks including, reduced costs and faster inflows when compared to check ordering, buying stamps, processing internally, and clearing bank channels" (Masson, 2001, p. 102). Reconciling time is decreased due to ACH payments being automatic, therefore making it easier to control payments and determine funds availability (Masson, 2001).

Small businesses can be a haven for fraudsters because most companies are not paying attention to the financial details (Carland et al., 2001). Internal and external fraud, theft, and unauthorized tampering with financial data are all valid concerns (Sharma, 2008). However, only a small portion of businesses report fraud activity. If reported, these incidents have both a positive and negative effect. The positive is that other businesses can see this as an opportunity to learn from each other. All will know what the fraud risks are and what measures could be helpful in detecting fraud (Hess & Cottrell, 2015). The negative effect results in the loss of

business, customer base, and lack of support from vendors and suppliers if they discover the incident (Hess & Cottrell, 2015). In addition to financial burdens, internal fraud has a tender attack on the business. It may appear to others that employees are not happy, and they turn to stealing to meet an individual need. Fellow employees are reluctant to report the bad activity they observe mainly because of fear or retaliation within the close fit environment (Hess & Cottrell, 2015).

Inevitably, smaller businesses have an advantage as they can be trusted advisors to their community of businesses. Although some of the fraud cases can be damaging, disclosure is helpful in building support and recovery.

Best practices for businesses

Some best practices businesses can use today as it relates to fraud protection services includes; reconcile daily based on any outstanding and paid checks; view all electronic transfer of funds; establish dual approvals; and implement separation of duties in place to strengthen internal procedures (Moore, 2018). Replace check writing with more ACH and wires services. Secure check stock, blank checks, signature stamps, and documents. Get in the habit of destroying paperwork if there is no longer a need for them (Masson, 2001). AFP recorded that 94 percent of companies lost their money because they did not have fraud protection in place (2016).

Other best practices a company can consider are being aware of others noticing the timing and frequency when someone from the business handles cash. Asking questions such as, when are the payables done? Who initiates wires and ACH transactions? Is there dual control for both services – where one person can initiate and the other can approve the transaction? Are

there appropriate protocols in place to send funds out securely? Make sure the staff is not rushed in doing the daily bookkeeping. If they were to get side tracked by an interruption it could be someone trying to distract them while the fraudster gathers information (Anderson et al., 2008). Be aware of the company vendor lists and keep them updated regularly. This will avoid any unusual invoices that may ask for unrecognized payments from accounts payable (AFP, 2016; Hess & Cottrell, 2015). Being knowledgeable of these tactics should ignite caution and awareness.

Training staff is important when protecting the business against the risk of occupational fraud (Moore, 2018). Although the best practices mentioned are not directly related to cash management solutions, the results could potentially improve the company's finances. The Association of Certified Fraud Examiners (2014) reported that insider tips caught 43 percent of all frauds (Hess & Cottrell, 2015). Therefore, encourage an environment of whistleblowers and commitment to detecting fraud.

However, on the bank side, it is highly recommended that companies who write checks invest in the positive pay service to protect their funds and provide accurate accountability to their bookkeeping (Masson, 2001). Exceptions found by the bank should be addressed immediately with the company to decide to pay or return (Masson, 2001). A consistent daily review will develop a behavior of helping the company mitigate check fraud.

The typical positive pay service can also match against the payee field, check number and amount of the check to detect altered checks (Masson, 2001). Also, teller positive pay will capture any stale dates or flag any checks that exceed the maximum dollar amounts allowed on the account (Masson, 2001). Reverse positive pay occurs when the bank transmits a file of the checks presented for payment to the company daily (Masson, 2001). The company matches this

file to its list of checks issued and notifies the bank of any items it wishes to have returned (Masson, 2001). Additionally, companies can also have a check block status to prevent any check disbursements whatsoever on an account (Masson, 2001). Fraudsters are crafty as they extract the numbers on the check and create an ACH transaction on the account. They will use this information to make online purchases or pay unauthorized credit card payments.

Businesses that have experienced ACH credit fraud increased from 7 in 2017 to 20 percent in 2018 (AFP, 2019). Over the past decade, ACH credit fraud has increased 4 to 13 percent signifying the heighten risk of online payments (AFP 2019). ACH debit fraud also increased from 28 percent in 2017 to 33 percent in 2018 (AFP, 2019). Much of the transactions were related to BEC scams.

When fraud occurs with a consumer's electronic transaction, the allocation of liability may fall on the business. As in larger security breach cases like Target Corporation, Chun states that "in the United States, there are no uniform federal laws related to business cybersecurity" (2019, p. 1). Therefore, as online retail sales increase to more than $500 billion by 2020, the expectation of breaches may trickle down to most businesses (Chun, 2019). Criminals use techniques such as account hijacking, identity fraud and theft, reserve phishing, insider organization fraud, and counterfeiting to access any form of payments companies collect (Anderson, et al., 2008; AFP, 2016).

Account hijacking happens when the fraudster uses customer credentials to access the origination system and use the information as if they were the account holder (Anderson, et al., 2008). The identity fraud uses information on social media and other websites that gives details about the individual within the company. Those individuals are targeted so that their identity can be obtained and used as the requestor in business email compromises (AFP, 2016). These types

of emails try to get someone off track from their daily task to invoke an immediate need to send money or other data to a fraudulent email. The email fraudster is after the account number and ultimately money. Reserve phishing appears to come from the Federal Reserve Bank with a phishing message that the bank is imposing restrictions on federal wire transfers (Kramer, 2015).

Finally, counterfeiting is one of the most creative fraud methods as the Internet gives room for fraudsters to copy and integrate their own payment systems into unsuspecting companies. The counterfeiter uses company look-a-like accounts, check stock, and signatures to create their own checks (Masson, 2001). Therefore, having positive pay service is so important. It will capture altered and duplicated checks right away.

Small businesses are not trained to keep a watchful eye on every area of their company. Most companies are spread thin when it comes to monitoring all facets of financial risk management (Hunter, 2011). They understand their daily operations and can control that part of the business well. However, when there is a fraud issue, they believe the bank will take care of it. If a bad check was cashed, they believe the bank will not pay for it out of their account. This is ***not*** exactly true. According to the UCC articles, if the item is identified within 30 days of the statement received, the bank may cover the loss to their customer (Masson, 2001). However, if the fraud happened beyond the 30-day timeframe, funds may not be recovered (Masson, 2001). Also, if fraud continues to occur on a business account several times, the bank may close the account and ask the company to leave the bank.

Companies that do operate with fraud solutions do so by authorizing the appropriate staff, with backups, to act responsibly with the finances (AFP, 2015). Again, there should be segregation of duties to help facilitate a secure environment (Carland et al., 2001). Business owners and internal staff should make others aware of the fraud gaps within the company

internally and externally (AFP, 2015). This means that every employee, vendor, customer, and those who are looking to exploit any weak security measures will be challenged before they are a detriment to the company (Hess & Cottrell, 2015). Business owners should take on the mantra that "unethical actions and fraud are intolerable" (Carland et al., 2001, p. 103).

As technology advances, so will small businesses be able to benefit from its enhancements. Protection from attackers will bring on more astute security measures. As mobile use has grown by 60 percent since last year, more consumers may use face ID technology as it is continuing to enhance security (Hodgson, 2018). Companies will use more two-step authentication processes to make payments and transfer funds (Hodgson, 2018). The future of mitigating fraud will become more innovative even for small businesses.

Conclusion

Every small business should develop a long-term strategy that includes protecting their company finances. Losses can be substantial to small businesses. While considering that companies do not fail because they are unable to pay debt, rather they fail because they are unable to stay liquid (Sharma, 2008). Having liquidity is critical to the lifeline of the financial success of the company. Going through steps to rule out vulnerabilities to risk and fraud is a procedure that should be done often. Businesses should take the time and allocate the resources to protect the company and avoid losses related to fraud. As technology advances, preventing internal and external attacks will continue to be a challenge to identify. However, it is just as important to understand the need for cash management fraud solutions and other techniques to assist in preventing losses. The new goal for the company is to minimize losses due to fraudulent activity. The solutions and best practices discussed in this paper will help avoid most

losses. Sharma (2008) postures a Greek proverb that appropriately says, “first secure an independent income, then practice virtue” (p. 72).

References

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. T*he Journal of Economic Perspectives,* 22(2), 171-192. Doi:10.1257/jep.22.2.171

Are you watching for these fraud blind spots? (2018, Apr). *Nonprofit World, 36*, 36. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/2048456190?accountid=11999

Association for Financial Professionals (AFP). (2015). Certified Treasurer's Council. Cybersecurity: Setting a cyberrisk management strategy. Retrieved from www.AFPonline.org

Association for Financial Professionals (AFP). (2019). Survey: Fraud hits record high, impacts 8% of businesses. *AFPonline.org.* Retrieved from https://www.afponline.org/ideas-inspiration/topics/articles/Details/survey-fraud-hits-record-high-impacts-82-of-businesses

Association for Financial Professionals (AFP). (2016). AFP Payments Security Guide: Trust but verify: How to stop business email compromise attacks. Retrieved from https://www.afponline.org/publications-data-tools/reports/guides/all-guides/Detail/trust-but-verify-how-to-stop-business-email-compromise-attacks/

Association of Certified Fraud Examiners (ACFE). 2018. Report to the nations: 2018 Global study on occupational fraud and abuse. Retrieved from https://www.acfe.com/report-to-the-nations/2018/default.aspx#about

Carland, J. W., Carland, J. C., & Carland, J. W. (2001). Fraud: A concomitant cause of small business failure. *The Entrepreneurial Executive, 6*, 73-108. Retrieved from

https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/2362 11285?accountid=11999

Hess, M. F., & Cottrell, J. H. (2016). *Fraud risk management: A small business perspective* doi:6149/10.1016/j.bushor.2015.09.005

Hines, C.; Hurtt, D.; Langsam, S. A. (2000). Shopping for Cash Management Services. *The Journal of Corporate Accounting & Finance*, Pages 15 – 19.

Holbrook, T. (2017). PayThink: Emerging payment tech levels the field for small businesses. PaymentsSource. Retrieved from https://www.paymentssource.com/opinion/emerging-payment-tech-levels-the-field-for-small-businesses

Hunter, M. G. (2011). Understanding the common causes of small business failures: A qualitative study. *Journal of Applied Management and Entrepreneurship, 16*(1), 86-103. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1415 791117?accountid=11999

Kramer, B. (2015). Trust, but verify: Fraud in small businesses. *Journal of Small Business and Enterprise Development, 22*(1), 4-20. Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/1655 518003?accountid=11999

Masson, D. J. (Ed.). (2001). Essentials of cash management (7th ed.). Bethesda, MD: Association for Financial Professionals.

Messmer, E. (2012). Most fraud against businesses from bad checks, not electronic payments. *Network World (Online),* Retrieved from

https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/940853723?accountid=11999

Moore, J. (2018). The relationship between organization size and occupational fraud. *International Research Journal of Applied Finance.* Vol IX (5), pp. 248 – 276.

National Automated Clearing House Association [NACHA]. (2019). Fed study confirms accelerating growth in ACH payments. *Targeted News Service* Retrieved from https://dbproxy.lasalle.edu:443/login?url=https://dbproxy.lasalle.edu:6033/docview/2166095621?accountid=11999

Prasad Das, C. & Parida, M. (2016). A Study on Cash Management and Determinants of Cash Holding. *Splint International Journal of Professionals*, Vol.-III, Issue-3, pp. 102 – 106.

Sharma, D. (2009;2008;2010). Working capital management: a conceptual approach. IN: Himalaya Publishing House. Chapter 4. Pages 72-91.

Small Business Administration. (2014). Office of Advocacy: Frequently asked questions.

Small Business Administration. (2019). Uniform Commercial Code. Retrieved from https://www.sba.gov/category/navigation-structure/starting-managing-business/starting-business/understand-business-law-7

Son, I., & Kim, S. (2018). Mobile payment service and the firm value: Focusing on both up- and down-stream alliance. *Sustainability, 10*(7), 2583. doi:10.3390/su10072583

Sullivan, R. J. (2014). Controlling security risk and fraud in payment systems. *Economic Review (Kansas City), p.* 47.

Tommasi, F., Catalano, C., Fornaro, M., & Taurino, I. (2019). Mobile session fixation attack in micropayment systems. *IEEE Access,* 1. doi:10.1109/ACCESS.2019.2905219

U.S. Small Business Administration Office of Advocacy. (2018). Frequently Asked Questions About Small Business. Pages 1 – 4. Retrieved from https://www.sba.gov/sites/default/files/advocacy/Frequently-Asked-Questions-Small-Business-2018.pdf