VARNEY CAREs

COMMUNITY • ACCOUNTABILITY • RELATIONSHIPS • EXCELLENCE

Varney & Associates, CPAs, LLC | 1501 Poyntz Avenue, Manhattan, KS 66502

Vol. 3 Issue 1 | February 2020

INSIDE THE ISSUE

What is business continuity?

By Richard Boggs

A lot of people mistakenly compare disaster recovery and business continuity as the same. This is not the case. Disaster recovery is how you recover from a disaster. Business continuity's scope includes disaster recovery, because not always is there a disaster when speaking about business continuity.

Business continuity is more than just backup and recovery, it involves thinking about all the processes and procedures companywide that could affect the business negatively.

Business continuity covers many different facets of each business and are typically not the same for each entity. However, the end goal is the same. Keeping the business alive and running when something unforeseeable does happen.

When it comes to the financial industry, there are several different categories that need to be paid attention to, and a full list of those categories a can be found in the Federal Financial Institutions Examination Council's (FFIEC) Business Continuity Management handbook from November 2019.

- Business impact analysis
- Enterprise wide Risk assessment
- Return time objective
- Recovery point objective
- Disaster recovery/business continuity testing objectives and requirements
- Third-party vendor expectations
- Management and Board interaction

Let's break these down a little bit so they are better understood.

Business impact analysis (BIA)

The business should list all the critical functions and departments that are necessary to keep the company running. Keep in mind this can sometimes be small things that businesses don't think about. For instance, internet connection, telephone connection, credit card machine, extra cash on hand, extra paper forms of things that may be completed electronically, etc.

Enterprise wide risk assessment (RA)

An RA will help identify potential risks to the company. This document isn't only covering what is needed for business continuity, but rather all risks for the entire organization. It should also list how high those risks are, how probable they are, what is being done to mitigate those risks, residual risks, what is being done for periodic testing to make sure those risks are being mitigated, and finally, the results of those tests, at a bare minimum.

Return time objective (RTO)

An RTO is how long the business believes it is allowable for a critical function or department to be completely down before being fully operational. This requires deep thought into all the processes around that function or department to identify all dependencies that go along with it.

Recovery point objective (RPO)

An RPO is what the business would consider an acceptable loss. It is the maximum targeted period in which data might be lost from a major incident. Ask yourself, how much data loss is acceptable? Zero might be the answer that comes to mind, however, is that always an obtainable goal? If you lost data for the last day, could it be recreated? Do you have other policies in place that allow it to be recreated? For example, we created an electronic document from paper, by scanning, then shredding the original. But is that document truly gone? Is it still in a shred bin? On someone's desk? There are a lot of intricate parts of an RPO.

Disaster recovery/business continuity testing objectives and requirements

What is the main goal of business continuity? Keeping the business operational when an event occurs. When creating a plan, we must think about want we want to see in our tests. Do we find it acceptable to perform tabletop only tests? Or do we want to test our policies/procedures by taking a system offline in order to see how we perform? When you find a fault in your test, it is imperative that you take corrective action because if you see it then, you WILL see it when a disaster really strikes. The business will also need to think about what are "acceptable testing results". Does the test have to be 100% to be acceptable? Or, can we recover 85% of a department and function well while we recover the last 15%?

Third-party vendor expectations

Personally, I think this is where I see the biggest misunderstanding when it comes to business continuity. If you have a third-party vendor that is hosting or performing a critical function for your business, then as a business, you need to make certain that all the above is true for that vendor. They also need to have a BIA, RTO, RPO, testing, RA so on and so forth. They need to provide you with those test results. If they allow it, take part in their testing and document what you found good and bad, and discuss with the vendor opportunities for improvement. Don't take a back seat and think that the vendor has you covered. Know they have you covered, because at the end of the day, a service level agreement doesn't protect your company from failure.

Management and Board interaction

Upper management and the Board of Directors should have transparency into what is going on. The Board should be approving the policies annually and expressing their concerns on the matter. They should also be involved in testing, from time to time.

Final Thought

This is, by no means a know all, end all document, but rather, high-level points that are imperative in your disaster recovery/business continuity plans. Make sure your business is covered and prepared for an event of this nature. It isn't a matter of IF; it is a matter of WHEN. While the FFIEC has much more detailed information in their handbook, we can help you in the design, development and testing of your plans.

Business Continuity includes, but is not limited to:

- *Optimizing processes and procedures, company-wide, that could affect the business negatively*
- *Third-party vendors are held to the same standards*
- *Remain aware of the information detailed within the FFIEC Business Continuity Management handbook from November 2019*

Richard Boggs
Information Technology Director

If your bank is considering its Business Continuity plans and need assistance, give Rich, or any one of the banking team members, a call at 1-800-240-5004. We can help design, development and testing of your plans.

Identifying Signs of Financial Elder Abuse & How to Help

By Jenn Hildebrand

There are many important people in our lives – our families, those we work with, or go to church with, our customer group, our neighbors, and friends. These people are of all ages and backgrounds. Some are more susceptible to be taken advantage of, especially when it comes to their finances and how they are handled and used. Elder abuse is a term used to describe this form of neglect as it relates to people in their later years in life. The Centers for Disease Control and Prevention defines elder abuse as "an intentional act, or failure to act, by a caregiver or another person in a relationship involving an expectation of trust that causes or creates a risk of harm to an older adult. (An older adult is defined as someone age 60 or older.)" Unfortunately, elder abuse is an area of concern for all financial institutions as it relates to financial abuse or exploitation. We can all do our part to help prevent this from happening to someone we know.

Family members, caretakers, neighbors, professionals, and con artists can all be responsible for committing elder abuse. It is estimated that older adults lose more than $36 billion every year to scams, fraud, and exploitation. What are some of the signs that a customer or someone you know may be the victim of some form of elder abuse with regards to their finances?

1. Caretakers that are unusually involved in the financial affairs of someone they assist, can be a sign of financial elderly abuse. It is unfortunately easy for these trusted individuals to threaten or abuse the elderly to get them to do what they want with their finances. Signs can include payments to caregivers or withdrawals that do not seem normal. Perhaps they trick or force them into taking out cash that the caregiver then keeps for themselves.
2. Joint accounts that are drained without the approval of the joint account holder. Unfortunately, joint account holders are often children, grandchildren, or other family members. A sudden change in the use of the account, such as a large increase in debits or transfers, can be a sign that a joint account holder is misusing the funds and taking advantage of the elderly person that added them to their account.
3. Internet and telephone scams are very often targeted at the more vulnerable elderly population. Not understanding how the Internet or e-mail works, puts the elderly at a high risk for being scammed. Examples may include e-mails requesting funds in order to receive an even larger settlement or to help a loved one in need, Facebook requests for money from someone claiming to be someone they are not, or phone calls telling the person they must pay a fee to receive a future amount. Oftentimes, the fraudulent fund requests are made via wire transfers.
4. New loans in the person's name that don't seem to make sense could be a sign of identity theft. For instance, why would someone living in a nursing home that only uses public transportation when running errands suddenly take out a car loan?
5. Unusual use of credit or debit cards should also be considered suspicious. This could include new debit card requests, online shopping activity that never existed before, the addition of someone authorized as a user on a card, or charges or purchases completely out of the normal for the customer. Gambling, dining out, shopping splurges, and so on are all examples of the possible fraudulent use of debit or credit cards.
6. Suspicious signatures on checks or other documents can be a sign of elder financial abuse. Another possible sign of fraud – bank statements no longer go to the customer's home. CDs are closed without regard to penalties.

If you identify signs of financial elder abuse, what can you do? How can you try to help someone who might need your assistance with regards to someone taking advantage of them and their finances?

1. Completing and submitting a Suspicious Activity Report (SAR) is a great idea if the activity meets the dollar threshold and other requirements of a SAR.
2. Consider contacting Adult Protective Services for your state. This service is for elderly persons living alone or in non-institutional settings. Adult Protective Services agencies coordinate efforts between social services, law enforcement, and other agencies to investigate allegations.
3. Exploitation for victims in a nursing home, typically by staff or other residents, can be reported to Adult Protective Services and/or your state's nursing home ombudsman.
4. For suspicions of identity theft, a Federal Trade Commission (FTC) identity theft report can be created. You can then take it to local law enforcement and file a police report.

5. Of course, if there is suspicion of immediate danger to the elderly person, you should call emergency services. Someone having their life threatened in any way if they do not withdraw money for and pay for items for another person, is an example of an emergency that can constitute the need to dial 911.

Elder abuse can go unreported for a variety of reasons. Identifying the abuse can be very difficult. Sometimes the elder does not answer your questions or understand what you are asking them. Remember, if you suspect financial elder abuse, report it. It is not your responsibility to judge whether abuse is taking place. Once you report abuse, the authorities have the training to investigate and address abuse allegations. With age, someone may go from making very sound financial decisions to making very poor ones. You do not have to try to determine what the cause of the change in spending habits are. Again, the authorities can investigate this.

It can also be a very difficult decision to turn in someone that you know or that the elder trusts and cares for. You must remember that if there is no abuse, the authorities will make that determination and the accused will be cleared. But, if financial elder abuse is occurring, the abuser may never stop unless someone intervenes. Keeping your loyalty with the vulnerable elder is the best decision in this case. If you are fearful of the abuser, you may be able to anonymously report your suspicions to Adult Protective Services. All threats should be reported to the police.

The only way we can help prevent elder abuse, is to do our part in identifying and reporting possible cases. Monitoring accounts for suspicious activity is an important step in financial institutions to help make this happen. Educate employees on ways to identify elder abuse. Without you and your involvement, the abuse will continue. Help protect your relative, neighbor, friend, or customer – watch for and report financial elder abuse.

BSA Corner: Banking & Hemp-Related Customers

By Amanda L. McKeeman

We have had many questions come our way regarding banking hemp customers versus banking marijuana-related businesses. When a Bank is required to file continuing Suspicious Activity Reports on their customer solely based on their line of business, this is important. In December 2019, the FDIC, FRB, OCC, and FinCEN released clarification pertaining specifically to hemp-customers. As part of the 2018 Farm Bill, hemp was removed from the definition of marijuana, and is no longer listed as a Schedule 1 controlled substance at the Federal level. Therefore, the regulatory agencies have determined Banks are not required to file Suspicious Activity Reports on hemp-related customers if they are reasonably certain that the customer is acting in accordance with applicable laws and regulations. Hemp-related customers are still subject to SAR reporting should suspicious activity be revealed through normal ongoing monitoring procedures. If your Bank chooses to provide services to hemp-related customers, policies and procedures should be updated to reflect the additional due diligence and monitoring that these customers require. It is critical that, if you choose to bank hemp-related businesses, the Bank has a clear picture of what the customer is producing or selling, and has assurance that it meets regulatory requirements in terms of chemical composition, etc. The Bank's policy should also address how the Bank will handle a hemp-related customer relationship should their product cross the line between legal and illegal based on the current regulatory guidelines. We will continue to keep you apprised of regulatory updates as the discussion of marijuana at Federal and State levels continue to progress. As always, if you have any questions or concerns relating to the ever-changing guidelines surrounding hemp and marijuana businesses and their effect on the Banking industry, please give us a call! We are here to help!

Jenn Hildebrand
Manager, CNAP

Unfortunately, identifying people struggling with financial elder abuse can be difficult. If we can provide further assistance, do not hesitate to contact Jenn or any one of the bank team members.

Amanda L. McKeeman
Senior Accountant, CPA

Federal and State laws regarding marijuana and hemp related businesses continue to progress. Banks should remain informed on current regulations as they are continuing to change. Let us know if we can help, through reviewing policies and procedures, or navigating the regulations, by calling Amanda or any one of the bank team members.

Community Bank Leverage Ratio

By Stephen Heimsoth

On September 17, 2019, the FDIC approved a final rule on the Community Bank Leverage Ratio (CBLR). The CBLR is the ratio of the tangible equity capital (tier 1 capital) divided by the average total consolidated assets of the qualifying community bank. To be a qualifying community bank a financial institution must meet the below criteria

- Has a CBLR greater than 9 percent
- Has less than $10 billion in average total consolidated assets
- Off-balance-sheet exposure of 25 percent or less of total consolidated assets
- Trading assets plus trading liabilities of 5 percent or less of total consolidated assets
- Not an advanced approaches banking organization

Reporting the CBLR is an optional election. A qualifying community bank can opt into the CBLR framework by completing the appropriate line items when completing the call report. If a Bank opts-in to report the CBLR and is a qualifying community bank, they will not be required to report or calculate risk-based capital. If a Bank opts-in, they may opt-out later but keep in mind, if the Bank opts-out they will need to start reporting and calculating risk-based capital again. Before deciding to elect in, the Bank may want to consider how difficult and burdensome the current risk-based capital rules are versus how difficult it would be to opt back out of the CBLR capital framework and restart calculating the risk-based capital ratios at a later date if it was ever decided to switch back. A Bank that opts out of the CBLR framework can subsequently opt back into the CBLR framework if it meets the qualifying criteria.

Effective date for this change is January 1, 2020, which means financial institutions can make the election to opt in to report the CBLR instead of risk-weighted capital starting on the first quarter call report for 2020.

If after opting in, a Bank fails to satisfy one or more of the qualifying criteria, the Bank is given a two-quarter grace period to either meet the qualifying criteria or to comply with the risk-based capital reporting. Take note, this two-quarter grace period applies for banks whose leverage ratio is below 9 percent but greater than 8 percent. If a bank's leverage ratio falls below 8 percent, they will not be permitted to use the grace period and must comply with the risk-based capital reporting.

A Change in Unauthorized Return – Reason Codes

By Stephen Heimsoth

Effective April 1, 2020 the return reason code R10 will be changed to "customer advises originator is not known to receiver and/or originator is not authorized by receiver to debit receiver's account" and should only be used for those transactions that are truly unauthorized. Return reason code R11 will be changed to "Customer advises entry not in accordance with the terms of the authorization." R11 will be used to return an entry where the originator and receiver have a relationship and an authorization to debit exists, but there is some other error such as, but not limited to, the originator debited the account for the wrong amount or earlier than authorized.

R11 will be considered an unauthorized return and should follow all unauthorized entry return rules including having a Written Statement of Unauthorized Debit (WSUD) form completed and returned within a 60-day timeframe.

Bank's should educate employees to ensure the correct reason codes are used for unauthorized returns after April 1, 2020. The Bank's may want to update their WSUD forms so that return reason code R10 is only referenced in the appropriate reasons and R11 is added to the appropriate reasons.

It takes less time to do things right than to explain why you did it wrong.

~ Henry Wadsworth Longfellow

Stephen Heimsoth
Manager, CPA, CRCM

Bank regulations can be confusing and complex. You aren't alone in this challenge. Know that we are there to help. Contact Stephen, or any one of the banking team members, at 1-800-240-5004.

Varney Tax Tips

SE Corporation Health Insurance – Not a Tax – Free Fringe?

By Laura Wenzke & Michelle Crow

As an S Corporation, if any of your employees own more than 2% of your business's stock, benefits like health insurance, dental insurance and long-term care are treated differently. Greater than 2% shareholders must include the cost of their insurance premiums paid by the company as income subject to Federal and State income tax. The premiums are then deductible for the company as a wage instead of as a fringe benefit. The shareholder-employee gets a deduction for self-employed health insurance premiums on their individual tax return. For this to work, the S Corporation must pay the premium on the policy and correctly report he amounts paid on the shareholder-employee's W-2.

IRS Required Minimum Distribution (RMD)

By Tonya Wilkerson

In recognition of the short amount of time after the enactment of the SECURE Act that financial institutions have had to change their systems for furnishing the RMD statement, relief is being provided. Under this relief, if a financial institution provides an RMD statement to an IRA owner who will attain age 70½ in 2020 (including by providing a Form 5498), then the Internal Revenue Service (IRS) will not consider such a statement to have been provided incorrectly, but only if the IRA owner is notified by the financial institution no later than April 15, 2020, that no RMD is required for 2020.

We are here to help with your tax issues – feel free to reach out to any one of our tax team members.

Laura Wenzke
Senior Manager, CPA

Michelle Crow
CEO/Owner, CPA

Tonya Wilkerson
Owner, CPA

Getting to Know Varney

Melissa Larson
Owner, CPA

In prior issues, we introduced you to a few new faces here at Varney. In this issue, our spotlight is shining bright on Melissa Larson, lead Owner of the financial institution practice. Melissa has worked at Varney for more than 15 years (she did leave briefly for one year but couldn't stay away). She also has more than 10 years of bank internal audit experience. Melissa isn't just all about public accounting; she is also an avid K-State football fan, attending games (when it's not too cold!), runner and fitness guru.

Melissa let us in on a few fun facts about her and we are passing them along to you!

Before joining Varney, what was the most unusual or interesting job you've ever had? *Nothing too unusual– waitressing, babysitting, accounting assistant…. You could consider working at Arthur Andersen interesting…the stories are true.*

What is your biggest achievement, personally or professionally? *Professionally – passing the CPA exam. Personally – running a marathon, both were painful.*

What is your guilty pleasure?
Chocolate and cookies, preferably combined, but I don't' feel very guilty about it.

What inspires you? What are you passionate about?
I think my biggest passions are my family and anything health related - I actually have a fitness nutrition certification, and of course, K-State athletics.

What kind of impact do you believe you have on others, people/companies? *I hope that I can help others be the best that they can be, or at least better than they were.*

What quality/characteristic is your strongest and hope others emulate? *My honesty*

What is one or two of your pet peeves?
People driving in the left-hand lane.

What is your motto or personal mantra? *Strive to be a better version of yourself than you were yesterday.*

What is one thing on your bucket list that you hope to do?
Watch the Chiefs play in the Super Bowl. I was in the stadium to cheer on the Chiefs and experience the win! It was a stressful but exciting game and well worth it all!