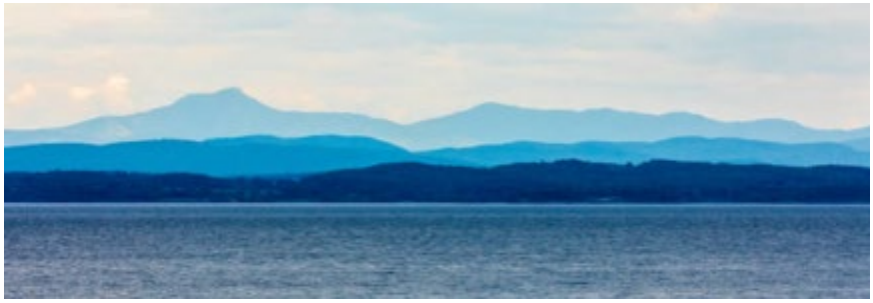
VERMONT
DEPARTMENT OF FINANCE AND MANAGEMENT

Summer 2020 - Internal Control News



The purpose of this quarterly newsletter is to provide agencies and departments with articles on good business practices, fraud prevention, and Internal Control responsibilities. Through articles intended to promote educational and professional development opportunities for employees, this newsletter seeks to raise awareness across state government on the importance of internal control. We hope that by providing you this array of information, we can keep you informed of internal control related activities, and help you implement and maintain effective controls in your areas of operations.

https://finance.vermont.gov

Volume 2 Issue 2

Our 2020 Self-Assessment of Internal Control (SAIC)

The *Internal Control Unit* will be e-mailing its annual **Self-Assessment of Internal Control** questionnaire to all agencies and departments by mid-July. Self-assessment aims to raise awareness of internal controls across Vermont State Government and is a catalyst for improving our internal control systems. The annual SAIC provides areas with a tool to review and document their current internal control practices, while helping management identify potential areas of risk or non-compliance within their organizations. Like prior years, agencies and departments will be given approximately 3 weeks to complete, review, and certify their questionnaire. F & M truly appreciates you and your staff's dedication and valuable time devoted to this important State of Vermont annual project review.

Helpful Web Links - Internal Control Standards

A Guide for Managers 2.0 **is available with other important linked resources:**

IC Standards Guide:
https://finance.vermont.gov/sites/finance/files/documents/Pol_Proc/IC/FIN-Internal_Control_Standards_Managers_Guide_Master.pdf

IC Website Resources:
https://finance.vermont.gov/policies-and-procedures/internal-controls

IC Questions? Contact:
jeffrey.montgomery@vermont.gov

Reminder: All Agencies and Departments

Maintain active registration in the System for Award Management

During the last few months, more than one state agency or department has experienced issues with applying for Federal assistance due to expired registrations. The issues were able to successfully resolve, but this has prompted us to remind all agencies and departments of this important annual task. In order to be eligible for Federal assistance, your agency or department must register its DUNS number on sam.gov and must renew its registration annually. While it may seem unnecessary to renew your registration if you're not currently applying for or receiving Federal assistance, the Department of Finance and Management recommends keeping all registrations active so that each agency or department is prepared for unanticipated situations and opportunities. It is important that each agency or department track which employees are designated as points of contact for the registration and transition this designation in the event of staffing changes. While the registration must be completed annually, updates to the registration may need to occur more frequently in order to keep current on the contact information.

Also, please be aware that as your active status nears its annual expiration, you may receive postcards or email reminders from a variety of sources offering to assist you with your renewal - for a fee. ***Please do not pay one of these services to assist you with your renewal***. There is no cost to register and the process is not difficult. Each agency or department is responsible for maintaining its own registration(s); however, if you have questions regarding this requirement please feel free to contact ***Cassandra Ryan, Statewide Grants Administrator*** at cassandra.ryan@vermont.gov. Please click the link below to bring you to the resource page where you can access more information regarding the registration process.

https://www.sam.gov/SAM/pages/public/help/samQUserGuides.jsf

State Fraud – During the Pandemic

F & M, Internal Control Unit present examples of fraud during COVID-19

- **Fraud during the COVID-19 pandemic and how to avoid it**
  By: Gabrielle Saulsbery, NJBIZ - May 20, 2020
  https://njbiz.com/fraud-covid-19-pandemic-avoid

  People are equipped with everything they need to avoid becoming the victim of fraud, according to United States Attorney for the District of New Jersey Craig Campeonato: all they need is common sense. If something sounds like a get rich quick scheme or something that's too good to be true, like a cure for COVID-19, that's probably what it is: too good to be true. "There's a dark underbelly of our society … that look at [how they can] take advantage of the situation," Carpenito said. "It's all about being diligent to avoid falling victim to those folks."

  Carpenito, Monmouth County Prosecutor Christopher Gramiccioni, Acting Insurance Fraud Prosecutor Tracy Thompson, and Acting Director of the Division of Consumer Affairs Paul Rodríguez spoke about COVID-19 related scams and the federal and state government's enforcement efforts to stop them in a Tuesday webinar hosted by Attorney General Gurbir Grewal. Price gouging, the sale of fraudulent personal protective equipment, and phishing scams have all been prevalent during the COVID-19 pandemic by bad actors. In some cases,

Carpenito said, PPE has been marked up 700 percent. That's the difference of a hospital system spending $2.6 million to purchase equipment to protect their workers compared to a fair price of $300,000. Prior to COVID-19, there were six main distributors of N95 masks in the country. The bad actors gouging the prices are among distributors who have come online since the start of the pandemic. Others have sold masks purported to be N95 that weren't actually, leaving people who think they're safe at risk of catching and spreading the virus. "This is not a one state problem, this is a 50-state problem. We have open investigations in 61 of 93 offices [nationwide], about 350 open investigations right now," he said. "A lot of stuff is being imported from overseas, [and we're] seeing major impacts in New Jersey and in Brooklyn, in California – cities where we have ports. We've seen this grey market pop up with a network of brokers that didn't exist prior to COVID-19." Gramiccioni noted that much of the fraud in Monmouth County is targeted toward the elderly community, or 20 percent of its population. Funds, a trusting nature from time's past, and limited experience in technology – they're not scientific, and not across the board, noted Gramiccioni, but they're three things that make a good opportunity for targeting. Gramiccioni addressed grandparent scams, when a scammer calls someone and says, "Grandma? Is that you?" and the person on the receiving end naturally responds, "Chris?" or whatever the grandkid's name is. Then they call, often at odd hours, often relating the call to the pandemic, with claims like "I lost my job. Can you wire me money?" "Scammers, they follow the news. They put a COVID twist on [scams]," Thompson said. "We used to get grandparent scams like 'I'm arrested' or something, but now they call saying 'I'm in quarantine.'" Proactive messaging is important, Gramiccioni said. The Monmouth County Facebook and Twitter pages update followers on common scams. "The goal is to have potential victims be hard targets. The goal is to try and get personally identifiable information. That's what drives a fraud," he said.

If a person is concerned someone asking for money or personal information on the other end of a phone call is a fraudster doing a so-called grandparent scam, Grewal suggests asking that person about a family pet or friend or reaching out to another family member before wiring money. "One of the fears I have is as recovery money begins to flow in, there's going to be a whole host of fraudsters that are going to try to take advantage of that," he said. People are not going to ask you for your social security or bank info over the phone for you to get the federal relief funds, he noted. Thompson noted that she anticipates an uptick in overcharging for medical services in the coming months, especially with increased telehealth services. "We recommend the insured takes 10 seconds to write down the length of the call and what happened and discuss how long it was and who you spoke with … Then you have a record, Thompson said. "Take notes and compare to an explanation of benefits. Even if you're not paying for it, we as a society are paying for it when there's fraud in the health care system."

- **The COVID-19 Epidemic As A Catalyst For Health Care Fraud**

Michael Adelberg & Melissa Garrido, May 7, 2020
https://www.healthaffairs.org/do/10.1377/hblog20200504.459546/full/

The combination of fear, loosened health care regulations, and expected stimulus payments in

response to the novel coronavirus disease (COVID-19) pandemic could unleash an unprecedented surge of health care scams and fraud. Allowing for flexibility in the health care system and an economic stimulus package are both reasonable responses to the ongoing crisis, but law enforcement and regulators must be vigilant for bad actors who exploit these responses to defraud consumers and payers. For decades, schemers have deployed ingenious consumer-facing scams and payer-facing fraud schemes that bleed the US health care system. Health care fraud in the US approaches $300 billion annually (of which the Department of Justice recovered $2.6 billion in 2019). Fraud hot spots tend to follow the money; recent hot spots include power wheelchairs and scooters, ambulance, counterfeit medicines, and "body broker" rings that ship people with addictions to fraudulent treatment facilities. Through the Coronavirus Aid, Relief, and Economic Security (CARES) Act, an estimated 140 million US households will soon have an injection of cash. This, coupled with the increased susceptibility to fraud that occurs with the fear many are experiencing, increases the chance that COVID-19 will be the newest consumer-facing fraud hot spot. Meanwhile, the Trump administration has taken a number of steps to relax long-established regulatory requirements and processes in the interest of increasing the capacity of the health care system to address COVID-19 and allowing distressed providers to focus solely on patient care. In so doing, unethical and fringe providers will have the opportunity to engage in wasteful and fraudulent activities in new ways. Law enforcement and regulators are gearing up to address consumer-facing scams, but they do not appear comparably focused on the coming wave of payer-facing fraud and waste.

Consumer-Facing Scams - *To their credit, the federal government's law enforcement and consumer protection organizations are expecting a wave of consumer-facing fraud. The US Attorney General recently sent a formal memo to all US attorneys directing them to focus on "detecting, deterring and punishing wrong doing" related to COVID-19. The Department of Health and Human Services (HHS) Office of Inspector General issued a COVID-19 fraud alert because "some bad actors are preying on people's fears for profit, perpetrating fraud schemes, including marketing fake COVID-19 test kits and unapproved treatments through telemarketing calls, social media platforms, and door-to-door visits." Similar statements were issued by the Food and Drug Administration (FDA), Federal Trade Commission (FTC), and several state attorneys general. Outside of government, the Better Business Bureau established a web page specifically for COVID-19 scams; it is warning consumers about price-gouging suppliers, low-quality medical masks, fake philanthropy raising money through crowd funding, and other problems. The media has also reported on consumer-facing COVID-19 scams, including articles and reports in the New York Times, Washington Post, Wall Street Journal, Reuters, Time, Forbes, ABC News, CNBC, and other sources.*

Action On Consumer-Facing Fraud - *There have been a handful of actions taken in response to consumer-facing COVID-19 scams. On March 9, the FTC and the FDA "jointly issued warning letters to "seven sellers of unapproved and misbranded products, claiming they can treat or prevent the Coronavirus." The FDA has issued 23 more warning letters since then. On March 22, the Department of Justice (DOJ) took its first enforcement action against a COVID-19 scammer, imposing a temporary restraining order and opening a criminal investigation against the operators of the website, "coronavirusmedicalkit.com." Three days later, the FBI made its first*

arrest. It arrested Keith Lawrence Middlebrook on fraud charges for alleging "he personally developed a 'patent-pending cure' and a treatment that prevents coronavirus infection." Prior to his arrest, Middlebrook posted a video of himself making extravagant claims of his product's curative power. Prior to the video being pulled down, it was viewed more than 633,000 times. Since Middlebrook's arrest, the DOJ has made a few more arrests. Beyond these few actions, law enforcement is actively surveilling and investigating numerous reported scams. According to a March 20 memo, the DOJ is aware of scams related to: fake COVID-19 cures being sold online; phishing emails under guise of communications from the World Health Organization or the Centers for Disease Control and Prevention; websites and apps that claim to share COVID-19 information to gain payment or receive personal information; and fake charities raising money. The New York Attorney General asked for public vigilance and information regarding "reports that individuals are knocking on doors" selling bogus COVID-19 tests. The Alaska Attorney General filed charges against an online seller buying respirators and flipping them on eBay and Amazon. Other reported scams include robocall work-from-home opportunities that solicit personal information and duct cleaners who claim their service protects people from COVID-19. In addition to focusing on consumer facing COVID scams, law enforcement is focusing on cases of hoarding and profiteering. On March 23, President Donald Trump ordered HHS and law enforcement to prevent hoarding and profiteering of medical supplies necessary for treating COVID-19. At least two actions have since been taken. On March 29, the FBI arrested Baruch Feldheim for coughing on officers while claiming he has COVID during a profiteering investigation. The next day, the DOJ announced the arrest of Erik Santos for offering "kickbacks in exchange for medically unnecessary tests—including potentially hard-to-obtain COVID-19 tests."

Limited Action To Address Payer-Facing Fraud And Waste - *Hoarding aside, there has not been corresponding attention paid to payer-facing health care fraud and waste opportunities. The COVID-19 epidemic has placed enormous stresses throughout the health care system. Congress, through the CARES Act, seeks to address these needs with additional money in the form of loans, grants, and increased Medicare and Medicaid funding. Meanwhile, the Trump administration has relaxed numerous rules and regulatory processes to increase the health care system's capacity and to allow providers to focus on patient care during a national emergency. Examples of the regulatory relaxations in Medicare and Medicaid include, but are not limited to, waiving and relaxing requirements regarding: signatures for certain health care services, prior authorization requirements, reimbursing for offsite services, provider enrollment rules, reimbursing services without a written physician order, increasing the range of reimbursable ambulance services, services and drugs from network providers and pharmacies, and audits of providers and health plans. Some of these flexibilities concern areas of known program integrity weakness. For example, 11 percent of excluded providers (barred from Medicare and Medicaid) are receiving Medicaid payments—a problem that will likely worsen with additional provider enrollment flexibilities. Improper payments totaled $45 billion in Medicare and $60 billion in Medicaid and the Children's Health Insurance Program in 2019 prior to these relaxations. These numbers may increase in light of the COVID-19 epidemic, which is estimated to cost Medicare an additional $38–$114 billion in the next year, even without considering the impact of regulatory relaxations.*

Looking Ahead - *There are compelling health policy arguments for relaxing regulatory processes and requirements during a national emergency; strong action is necessary to address the COVID-19 crisis. Yet, while leaders across the federal agencies are focused on consumer-facing COVID-19 scams, there is not yet corresponding concern on payer-facing fraud and waste. Preventing fraud and waste is more efficient than recovering improper payments. Affirmative statements from agency leaders that the federal government is watching might deter some bad actors. After the surge of COVID-19 infections pass, the Centers for Medicare and Medicaid Services and state Medicaid programs should conduct outlier analyses to identify areas where fraud and waste probably occurred; targeted auditing and investigation will be warranted. The overwhelming majority of health care providers have high integrity, and many are risking their own health to care for others with COVID-19. But history suggests that bad actors take advantage of leniency, and agency leaders have just offered great leniency. We hope to remind them about the bad actors.*

- **Unemployment fraud claims continue to skyrocket during COVID-19 pandemic**

by: Jessica Bruno, OKLAHOMA CITY (KFOR) May 11, 2020
https://kfor.com/news/unemployment-fraud-claims-continue-to-skyrocket-during-covid-19-pandemic/

Several people have now reached out to News 4 after receiving unemployment funds on a debit card after never actually filing for unemployment. "At first, I thought it was just junk and then when I seen y'alls story, I got a little worried," Dave Brown told News 4. Brown is talking about an unemployment debit card from the Oklahoma Employment Security Commission that he received in the mail. "I just cut that up thinking it was junk mail and I shredded the document that came with it," he said. That's because he said he's never filed for unemployment. So, he contacted OESC. "I talked to a couple of people and they gave me one phone number that just gave me an email address," Brown said. He emailed the address and he said someone got back to him saying they were looking into it. Brown isn't alone. News 4 heard from several others Monday who also received a debit card out of the blue when they shouldn't have. "This is very large scale and has multiple layers to it," Brook Arbeitman with the Oklahoma State Bureau of Investigations said. OSBI has now stepped in, creating an Unemployment Fraud Task Force. "We've dedicated a lot of resources to it from agents who are going to be dedicated to investigating the claims, to analysts who are trying to put all the dots together," she said. Along with cases like Brown's, a lot of that is focused on letters that have been piling up at businesses, filled with names of people trying to collect unemployment even though they never worked for that company. "We are going to track down and put a stop to any of these crimes that originating in Oklahoma, but we're aware from our federal partners that some of these may be generated out of state," Arbeitman said. "We're just not going to tolerate Oklahomans being taken advantage of during this time."

F & M Staff Happenings: No staff changes for this quarter.

Internal Control News is published quarterly in the ***Spring, Summer, Fall,***
and ***Winter*** by The Department of Finance and Management, Internal Control Unit.
Please contact jeffrey.montgomery@vermont.gov with comments or suggestions.

Our latest F & M - Organizational Chart

https://finance.vermont.gov/about-department