Navigating scams, cybersecurity, and open meetings during the COVID-19 crisis

As the coronavirus public health crisis continues to impact the state, Colorado Attorney General Phil Weiser and the Department of Law have issued warnings and advice for consumers, businesses, and public entities.

Scammers often follow headlines, especially during a crisis, so we all need to be vigilant to protect ourselves and others. The Department of Law received more than 900 consumer complaints related to COVID-19, demonstrating how bad actors are seeking to take advantage of Coloradans.

As scam risks increase, so do cybersecurity threats. While people are working remotely, they may be more susceptible to these threats, which is why it is even more imperative that businesses and organizations follow cybersecurity regulations.

The COVID-19 pandemic has also impacted public-facing boards and commissions, but that does not mean they cannot conduct business while working remotely. Open meetings can be held virtually if the law is followed in regard to public access and notice of the meetings.

How consumers can avoid scams related to COVID-19

Scammers have been using fake phone calls, emails, texts, and social media posts to lure consumers into paying for non-existent coronavirus tests, prevention or treatment drugs, and personal protective equipment such as masks and gloves. Sometimes they direct unwary consumers to phony websites to steal important personal or financial information. They also hope to take advantage of our residents by using relief checks the federal government is sending to many Coloradans as part of the federal CARES Act to encourage people to steal bank account numbers or other sensitive personal information.

As Attorney General Weiser has warned, scammers take advantage of natural disasters and emergencies, but by working together we can protect ourselves and others.

”By learning how to avoid scams related to COVID-19, we can work together to ensure no one in our state is taken in by these malicious attempts to defraud Colorado consumers during this public health emergency,” he said.

The following are ways to avoid COVID-19 scams:

- Be wary of online offers for vaccinations. There are currently no FDA approved vaccines, pills, supplements, potions, lotions, lozenges, or other prescription or over-the-counter products available to treat or cure COVID-19.
- Don’t respond to texts and emails about checks from the government. For more information about stimulus checks, go to www.irs.gov/coronavirus/economic-impact-payments.
- Know that no state or federal government agency will ever call to ask for your Social Security number, bank account, or credit card number, or ask you to pay any fee or fine with a prepaid gift card or wire transfer. They will certainly never ask you to pay anything up front to receive a stimulus check. Anyone who does so is a scammer.
- Don’t click on suspicious links contained in unexpected emails or texts, or any other communication from unfamiliar sources. Those links could direct to a phishing website to steal personal or financial information or download viruses onto their computer or device.

- Check websites and email addresses offering information, products, or services related to COVID-19. Be aware that scammers often use addresses that differ only slightly from those belonging to the entities they are impersonating. For example, they might use “cdc.com” or “cdc.org” instead of “cdc.gov.” For the most up-to-date information on COVID-19, visit the websites for the Centers for Disease Control and Prevention (cdc.gov) and World Health Organization (who.int).
- Phony charity sites or people asking for donations in cash, by gift card, or by wiring money, should not be trusted. Do not be lured by “urgent” appeals. Before you make any donation, check the validity of charities by going to www.charitynavigator.org or www.charitywatch.org.

The Department’s Consumer Protection Division has been in contact with representatives from various online retailers like Amazon to coordinate efforts to address potential extreme price gouging on items such as paper products, cleaning supplies, hand sanitizer and soap, and other goods. It is important for Colorado consumers to remain vigilant and report any scams. With these reports, the Department will be able to work with other law enforcement agencies, including on a national level, to protect Colorado consumers and stop fraudsters.

If you see any scams, fraud, price gouging, or other attempts to take advantage of Coloradans during this public health emergency, contact Stop Fraud Colorado at 800-222-4444 or www.StopFraudColorado.gov.

Why following cybersecurity laws is vital, including when working from home

Colorado’s consumer data protection laws require companies and government agencies to protect the personal identifying information they collect and maintain and provide notice when there has been a data breach. These laws must still be followed, even as many businesses have transitioned to working from home.

Steps the law requires entities to take to protect personal identifying information that they maintain, own, or license

Any person, commercial entity, or governmental entity that maintains, owns, or licenses personal identifying information of Colorado residents in the course of its business, vocation, or occupation are required to take reasonable security measures to protect personal identifying information, taking into account the nature and size of the business and the type of personal identifying information they are collecting. See C.R.S. § 24-73-102 for more information for governmental entities, and C.R.S. § 6-1-713.5 for individuals or commercial entities.

Requirements for disposal of personal identifying information

People, commercial entities and government entities that maintain, own, or license personal identifying information in the course of their business, vocation, or occupation are required to develop and implement a written policy to ensure it is destroyed when it is no longer needed. See C.R.S. § 24-73-101 for more information for governmental entities, and C.R.S. § 6-1-713 for individuals or commercial entities.

What is required in case of a security breach

In case of a security breach—the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information—the person, commercial entity, or governmental entity, maintaining that information must conduct a prompt, good faith investigation to determine the likelihood that personal information has been or will be misused. Unless the investigation determines that the information has not been misused and is not reasonably likely to be misused, they also must provide notice to the affected Colorado residents.

That notice must be provided in the most expedient time possible, without unreasonable delay, and within 30 days after the date of determination that a security breach has occurred.

If the security breach is reasonably believed to have affected 500 or more Colorado residents, notice must also be provided to the Colorado Attorney General in the most expedient time possible and without unreasonable delay, but not later than 30 days after the date of determination that a security breach occurred. See C.R.S. § 24-73-103 for more information for governmental entities, and C.R.S. § 6-1-716 for individuals or commercial entities.

Notice to the Attorney General should be sent to the Consumer Protection Program Manager at databreach@coag.gov.

For more information about Colorado's data protection laws, go to https://coag.gov/resources/data-protection-laws/.

The Colorado Open Meetings Law and virtual meetings

The Colorado Open Meetings Law (COML) allows for virtual meetings to be held, and the Department is providing guidance based on both this law and the Colorado Administrative Procedures Act to state agencies about best practices. Go to bit.ly/OpenMtgsFAQ for more information.

Virtual meetings

The COML recognizes that "meetings" of public bodies may be conducted "by telephone, electronically, or by other means of communication." § 24-6-401(1)(b). The law provides that all "meetings" at which two or more members of a state public body, or three or more members (or a quorum) of a local public body, discuss "public business" must be "open to the public at all times." § 24-6-402(2)(a). A meeting accessible only electronically, such as by webinar, online video conference (e.g., Zoom), or telephone conference, complies with the COML so long as the means to access the meeting electronically are made available to the public.

The law also authorizes local public bodies to use electronic-only posting of notices of their meetings. § 24-6-402(2)(c)(III). For state public bodies, the statute requires that there must be "full and timely notice to the public." State bodies should adopt a 'flexible' standard that considers the interest in providing access to 'a broad range of meetings at which public business is considered,' as well as the public body's need to conduct its business 'in a reasonable manner.'" (*Benson v. McCormick*, 195 Colo. 381, 383, 578 P.2d 651, 652 (1978)).

Converting an in-person meeting to an electronic-only meeting

Under the existing law allowing for flexible standards in connection with notices of public meetings, it is permissible for a public body to amend a previously posted notice of a public meeting. *Town of Marble v. Darien*, 181 P.3d 1148, 1152 (Colo. 2008). Amendments can include the addition of new topics,

changes in the location of a meeting, or the means of accessing the meeting, but the COML requires at least 24 hours' notice for public meetings of local public bodies. § 24-6- 402(2)(c)(I).

While there is no similar provision for state public bodies, 24 hours' notice should be sufficient for a public meeting of a state public body, especially if there are extenuating circumstances that warrant a short notice period. Providing notice for more than 24 hours is appropriate where feasible. In addition, it is also important to consider whether a particular public body's statute, ordinances, charter, or rules require more than 24 hours of public notice. If so, then the more specific notice provision will control over the general provision in the COML.

Public comment

The COML does not require a "public comment" period, or any other form of public input during a public meeting. Rather, the purpose of the statute is to allow the public to observe, not necessarily to participate. § 24-6-401. Note, though, that many local public bodies do have such requirements in their ordinances or rules. If that is the case, the public body will need to use a technology for its electronic meeting that facilitates a public comment period.

Many current virtual-meeting services readily enable this function. The body may alternatively rely on the "chat" or similar functions of online video-conference systems such as Zoom or Skype, which allow participants to send comments to the body in writing.

How to set up electronic-only access for an executive session in conjunction with a meeting of the public body

If the public body uses a commercial internet-based video conferencing service such as Zoom, the service will allow for the creation of side-bar meetings into which selected participants may join the portion of the meeting that has been closed to the public. This will allow for the public meeting portion of the electronic meeting to remain open while the executive session is conducted.

Otherwise, in the absence of a commercial video-conferencing system, the safest way to conduct a closed executive session during a body's meeting is by having a two-mode method for accessing the electronic meeting. That is, if the meeting is conducted by both webinar and a concurrent telephone dial-in conference bridge, the webinar portion of the meeting can be suspended or recessed while the executive session is conducted by telephone. Once the executive session is completed, the body's board members would then rejoin the webinar video conference.

This article originally appeared in the June 2020 edition of *Colorado Municipalities*. Reprinted with permission from the Colorado Municipal League.