Cannabis Control Division

January 5, 2024

Dispensary Scams

Dear Licensees,

Happy New Year!

It has come to the Cannabis Control Division's (CCD) attention that there has been an increase in scammers contacting cannabis businesses and posing as either the electric company or the water company. Often, they are threatening to shut off services to exploit licensees for credit card numbers or payment information. Please be advised, and exercise caution when receiving questionable calls or text messages from persons claiming to be utility companies as they may come off as authentic. For your safety and security, we suggest you review the list of scam tactics below that have been previously reported to the CCD:

- Requesting employees download a private encrypted (untraceable) application to communicate through such as Signal or the employee's personal cell phone.
- Reporting a pending inspection.
- Requesting employees take photos of fire extinguishers, emergency alarms, exits, safes, cash, and marijuana products.
- Impersonating CCD compliance officers to exploit sensitive information or gain access to facilities.
- Impersonating an owner, manager, or their attorney instructing employees to deliver cash from the business to a location off-premises (frequently a hospital parking lot) or to make a cash deposit into a Bitcoin ATM.
- Impersonating law enforcement officers (FBI, DEA, etc.) investigating counterfeit currency deposited at the business with further instruction to acquire prepaid purchase cards and disclose the card numbers over the phone or to deliver $20 denomination bills to inspect for "authenticity".
- Impersonating law enforcement officers (FBI, DEA, etc.) investigating counterfeit currency resulting in the business's frozen bank accounts with further requests to deliver currency to an off-premises location for inspection.
- Impersonating a cannabis industry supplier requesting to inspect the premises.

All licensed employees must be vigilant to prevent these fraudulent attempts from becoming successful. Educating employees and preparing additional security measures is paramount. Be sure to verify personnel claiming to be CCD compliance staff. CCD compliance officers should be able to present an identification badge upon request, and the names of all compliance officers are listed on the CCD website. Also, business owners should create a protocol for the legitimate transfer of funds. Additional security measures may include creating a code word to authenticate valid requests for cash transactions from owners and managers. NEVER disclose any personal information, i.e., social security numbers, date of births, or credit/debit card numbers. All suspicious activities should be reported to local law enforcement for investigation.

Below are links to resources to report or verify scammers:

- Report scammers posing as FBI agents by filling out the following form: https://www.ic3.gov/
- Report scammers posing as DEA agents by filling out the following form: https://www.dea.gov/stories/2019/2019-06/2019-06-11/alert-extortion-scam-targeting-dea-registrants
- Report scammer calls posing as CCD to the Federal Communications Commission by filling out the following form: https://consumercomplaints.fcc.gov/hc/en-us/articles/115002234203-Unwanted-Calls-Phone-
- Contact the Cannabis Control Division for Compliance Officer verification: cannabiscontrol@rld.nm.gov

Thank you for your attention to this matter.