QUADSCORE INSURANCE SERVICES
BEST PRACTICES

FRAUD PREVENTION

Fraud & the Cannabis Industry

Due to the high-profile nature of the emerging U.S. cannabis industry, operators continually find themselves the target of both well-established fraud schemes, such as phishing & ransomware, and more industry-specific scams that take advantage of the large amounts of cash often collected at retail operations.

The following tips are meant to assist operators in educating their employees on how to avoid these common pitfalls.

Sample Fraud Schemes

Scheme 1: Impersonation of Authority

- **Initial Contact**: The scammer contacts an employee, typically at a lower level, via phone call or text message.
- **Impersonation:** They pretend to be a manager or high-ranking official within your organization.
- **Urgent Request**: The imposter convinces the employee that there is an urgent need to withdraw a specific amount of cash.
- **Transfer Instructions**: The employee is instructed to transfer the cash to an important person through a Bitcoin machine. Once deposited, the money is forever gone as the Bitcoin ledgers are not traceable and there is no financial intermediary.

Scheme 2: Impersonation of Vendor or Business Partner

- **Fake Email**: The fraudster sends an email to the insured, posing as a vendor or business partner, using a fake email address that closely resembles the legitimate one.
- **Change of Bank Account**: The email states that the vendor/partner's bank account has changed and instructs the insured to wire future payments to the new (fraudulent) account.
- **Unnoticed Discrepancy**: Because the fake email address is very similar to the real one, the insured often does not notice the difference and wires the money to the fraudster.

How to Protect Your Business & Employees

- **Verify Identity**: Always verify the identity of anyone requesting cash withdrawals or wire transfers, especially if the request is unusual or urgent. Use official channels to confirm the request.
- **Check Email Addresses**: Carefully inspect email addresses for slight discrepancies, especially when financial transactions are involved. Contact the vendor or business partner directly using known contact information to verify any changes.
- **Educate Employees**: Inform your employees about these fraud schemes. Make sure they know that legitimate requests for changing bank account details will follow proper protocols.
- **Establish Protocols**: Set up clear protocols for verifying and approving financial transactions. Ensure all employees are aware of these protocols.
- **Report Suspicious Activity**: Encourage employees to report any suspicious communications or requests immediately to their supervisor or the designated fraud prevention officer.