



Handling Phone Threats & Social Media Conduct

April 21, 2025

What & Why

Handling Phone Threats

- Several Stores have recently received threatening phone calls from scammers.
- Review the information on page 1 to ensure Our People are prepared to handle phone threats.

Social Media Conduct

- There have been instances of employees acting as a company representative on social media.
- Review the information on page 2 to ensure Our People know their role on social media.

IMMEDIATELY SHARE THIS INFORMATION WITH YOUR TEAM

Phone Threats

Please be aware of a scam that has recently occurred in several stores. This involves the steps and demands described below, or something similar.

- A person calls the store and demands an employee gather items such as medical supplies, towels, etc. Sometimes the caller first requests a Spanish-speaking employee.
- The caller then makes a threat of some kind. This threat may be a claim that this is cartel related, may describe current details of the store (to show they are watching), or even show themselves outside of the store with a weapon. They may also threaten to harm someone if the request is not completed in the allotted time frame.
- The caller may also demand the employee drive to a nearby store to purchase additional supplies such as gift cards or to wire money to an account.
- At this point, the caller may even threaten the employee by stating they have their personal information now and not to inform the authorities.

Using these tactics these individuals are first trying to elicit your sympathy, and then add a sense of urgency, followed by a threat to get the employee to eventually hand over or send cash.

If you encounter this situation: hang up and call 911 immediately, followed by your AVP.

If possible, also:

- Write down the telephone number of the caller, refrain from responding, and hang up. Provide the number to police.
- If possible, block the phone number or refrain from answering follow-up calls.
- Do not provide personal or financial information about you or the business.
- Never agree to meet with the caller.
- Do not return calls to the scammer or use any contact details they may provide.
- Do not respond to texts, emails, or social media messages. If you do, scammers may escalate their intimidation and their attempts at gaining compliance.
- Do not send money, gift cards, bank card details or online account information to anyone you do not trust.

Be sure to submit a security incident report via the Claims portal on the KC (select Security/Work-place Violence Incident).

Social Media Conduct

There have been instances of customers posting their negative in-store experiences publicly on social media platforms. It is important that no employee attempts to contact these individuals as a company representative.

- If an employee sees a social media post that is (potentially) damaging to the company, do not engage with the post in any manner (like, comment, direct message). There are processes and procedures the company has in place to address such an incident. It's possible that replying can make a situation unintentionally worse which can escalate to threats to store personnel.
- It is the employee's responsibility to pass along the post to their Store Manager and AVP, thus, ensuring it is escalated to the correct individuals to address the incident.

Note: It can be hard to know for sure if the incident is valid or not, as well as if the details are accurate or fabricated to push a false narrative. The best thing for Our People to do in this event is to refrain from any engagement of the post, the individual, or the comments.

If possible, also:

- Take a screenshot or screen recording of the post if it is removed from the platform.
- Avoid sharing the post with more individuals than necessary as social media platform algorithms will boost the post's visibility by putting it on more 'for you pages'.

If you are unsure if a social media post you come across should be escalated, always err on the side of caution and alert your leadership.

Final Steps

- 1. Acknowledge that you have shared this information with your team.
- 2. Sign and submit the IAM survey.

Published on: 4/21/2025