



**April 21, 2025**

## Handling Phone Threats

- ## Social Media Conduct

- ## IMMEDIATELY SHARE THIS INFORMATION WITH YOUR TEAM

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

[illegible]

## 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.