Fraud, Scams, & Phishing

As an employee of Chicago Scoops, LLC & Cold Stone Creamery, you will encounter a variety of customers and situations that will require you to use your absolute best judgement. To protect you as our employee and to protect Chicago Scoops, LLC's property, please review the below points as to how you should handle suspected fraud & scams both in person, over the store e-mail, or phone. Though the scenarios detailed below can be frightening, it is imperative that you are prepared to handle the potential situations accordingly, both for the safety of yourself, your team, and your store.

Please be advised that scammers often conduct location-based research ahead of time. **Do not disclose any company information to unknown individuals**. Instead, please direct them to our corporate office phone number 312-755-3723 or to our website www.chicagoscoops.com. **If an individual is physically threatening or intimidating you via the phone or in person, please call the police immediately.**

If you are approached, in person or via phone call, by a vendor or seemingly authoritative figure who demands compensation in either cash from the store or anything of value such as gift cards on the spot, please notify the corporate office immediately. Cash should only leave the store under two circumstances; 1) when being deposited into a Chicago Scoops bank account or 2) for paid-out related items such as milk and banana (note that paid outs more than $25 require supervisor approval). Scams can take many forms, some common examples;

- posing as a vendor or utility provider demanding immediate payment and threatening to cutoff services or supplies. Simply state that we do not process any payments at the store level and contact the back office immediately.
- posing as an authoritative figure/law enforcement – often these scammers will call in and not present themselves in person, they may know the names of staff, supervisors, and back-office staff, all of which can be obtained through publicly available information. Actual law enforcement officers will always have a legitimate ID/Badge verifying their identity as law enforcement and will never ask for compensation on the spot.

***Phishing**: When a fraudster tries to get private information via an email or a website. These details would allow them to access your account or computer.* **Phishing emails and text messages may look like they're from a company you know or trust.** They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, an online store, or a Chicago Scoops employee.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may:

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- offer a coupon for free stuff

Watch out for…

- Emails requiring you to click on a link and drive you to a webpage that looks like a legitimate institution.
- Alarming messages saying your account will be locked unless you act.
- Unexpected messages branded with corporate headers that upon inspection have typos and misspellings.
- Website URLs without HTTPS:// or the closed lock symbol next to it. When in doubt, type in the trusted URL.

Chicago Scoops, LLC
1901 N Clybourn Avenue, Suite 401, Chicago, IL 60614
P: (312) 767-2051

What To Do if You Suspect a Phishing Attack

- If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: **Do I know the company or know the person that contacted me?**
- **If the answer is "No,"** it could be a phishing scam. Look for signs of a phishing scam. If you see them, report the message, and then delete it.
- **If the answer is "Yes," report it to your supervisor** who can contact the company using a phone number or website we know is real, not the information in the email. Attachments and links can install harmful malware.

Watch out for…

- Receiving an unexpected call. If you're suspicious, hang up and notify your supervisor.
- Callers asking to verify private information or company structure, don't reveal this info.
- Urgent calls stating your utilities will be suspended or accounts will be closed.

Not limited to email or phone, attacks can come in the mail and **in person. It is better to be wary and cautious. If something seems off, **report it!** Especially when it comes to in-person threats, remember that you will never be asked to pay a vendor with cash without prior heads up so keep the money in the registers.

Failure to report suspicious activity to the appropriate supervisor or misappropriation of Chicago Scoops LLC assets may result in disciplinary action up to and including termination.

By signing below, I acknowledge my understanding of the Fraud & Scams policy laid out by Chicago Scoops, LLC.

Signature: _____

Date Signed: _____

Chicago Scoops, LLC
1901 N Clybourn Avenue, Suite 401, Chicago, IL 60614
P: (312) 767-2051