

From: Virginia Board of Pharmacy

Date: May 17, 2022

Subject: Healthcare Distribution Alliance Pharmaceutical Cargo Security Coalition Warning on Fraud Incidents



Board of Pharmacy

Healthcare Distribution Alliance Pharmaceutical Cargo Security Coalition Warning on Fraud Incidents

Healthcare Distribution Alliance Pharmaceutical Cargo Security Coalition (PCSC) is updating the [warning to the pharmacy industry, issued earlier this year](#), regarding product ordering/recall fraud incidents, several of which have resulted in losses. To update licensees of current trends, PCSC notes that attempts at fraud are persisting and that law enforcement and corporate security investigations into these incidents continue on multiple levels.

Some details regarding the schemes include:

- The perpetrators continue to convince distribution representatives (both in wholesale and retail environments, as well as over the phone and electronically) that they are making legitimate inquiries about drug shipments.
- The credentials the perpetrators are supplying are real, having obtained them through a variety of social engineering techniques.
- A fair number of retail pharmacies are now receiving telephone calls from individuals identifying themselves as being from a state board of pharmacy or a state health department. In these scenarios, the person calling (who is almost always female) asks the pharmacy representative for specific routine and disarming information, such as address, hours of operation, phone numbers, principal contacts, etc.
- The names used by the female callers to identify themselves include "Julie McNeil," "Cynthia," "Beth," "Beth Walton," and "Danielle."
- The caller eventually asks questions about the names of the pharmacy's primary and secondary wholesalers, the type(s) and cadence of their business interactions with their wholesalers, and, in some instances, account numbers.
- On some calls, the perpetrator uses the excuse that the board of pharmacy needs such information because it is responsible for notifications of recalls.

According to PCSC, this type of probe is an initial form of social engineering that gives the perpetrators what they need to take their inquiries to the next level. If they are unable to get the information they want during the initial call, they will use what they learned to impersonate the pharmacy's principal distributor (

because they now know who it is) in a subsequent call to again try to elicit account numbers and passwords.

If a licensee receives such an inquiry, PCSC suggests the following:

1. Do not answer any questions;
2. Indicate to the caller that someone will call them back;
3. Try to get a name and callback number;
4. Hang up; and
5. Immediately contact the pharmacy's known principal contact at the board of pharmacy or health department to report the incident.

In addition, PCSC requests such activity be reported to cforsaith@hda.org so it can be shared with law enforcement.