FRAUD ALERT: DISTRIBUTOR/CUSTOMER PRODUCT ORDERING SCHEME

Version 2 (Updated June 2022)

PCSC

HDA Pharmaceutical Cargo Security Coalition

BACKGROUND

Since December 2020, there have been reports of both distributors as well as several of their pharmacy customers receiving telephone calls and/or emails as part of a sophisticated "phishing" scam to unlawfully divert pharmaceutical goods in transit.

These scams are not new. Once largely focused on trying to obtain products related to diabetes testing and treatments, the attempts now include prescription medications and medical devices.

The individuals making the calls identify themselves as employees (or affiliates) of a particular distributor or of the pharmacy customer to secure account and other sensitive information, including: specific account information, account login credentials, employee names associated with accounts, contact email addresses and/or a pharmacy's federal or state license number. The scammers ultimately use that information to engineer the diversion of products as a misshipment — or the false reclamation of a defective product.

The illicit tactic used is known as "social engineering," or the use of deception to manipulate individuals into divulging confidential corporate or personal information that may be used for fraudulent purposes. Criminals use social engineering tactics because it is usually easier to exploit the natural inclination to trust than it is to decipher ways to hack into a company's IT systems.

The pharmaceutical and healthcare products most recently targeted have included anti-depressant, blood thinning, arthritis and HIV drugs as well as AED defibrillator machines, stethoscopes and blood pressure monitors.

METHODOLOGY: PHARMACIES

There are several methods being used to scam pharmacy customers. In one of the most recent scenarios, the scammer will telephone a pharmacy and pretend to represent the state's Board of Pharmacy or Board of Health. In those scenarios, the person calling (many times, a female) asks the pharmacy representative a number of questions — several of which begin as routine and can be characterized as disarming, such as: confirming the pharmacy's business address, hours of operation, phone numbers and who the principal contacts are, among others. It isn't long before the caller eventually asks questions such as the names of the pharmacy's primary and secondary wholesalers, the types and cadence of their business interactions with their wholesalers; in some instances, the caller asks for account numbers and account passwords. On certain calls, the perpetrator uses the excuse that the Board of Pharmacy needs such information because they are responsible for notifications of product recalls.

Another method the scammers will use is to pose as a manufacturer. In this version of the scam, the perpetrator will initially telephone a pharmacy and report a product issue that is stated to be the manufacturer's responsibility. The scammer informs the pharmacy representative that certain products they have recently received may need to be replaced but, if that becomes the case, a credit will be issued through the original distributor.

The scammer (still acting as a manufacturer representative) then requests the pharmacy's distributor account information to be able to issue such a credit. The scammer further informs the pharmacy that the distributor has verified this process through the manufacturer.

Finally, the bad actors may attempt wire fraud. They will contact pharmacy customers, again pretending to be a distributor representative, and request to change traditional payment methods, such as asking the customer to send payment to a new or unfamiliar wire account.

All types of pharmacies have been targeted in these scams — large country-wide commercial operations, small-town single proprietor businesses and, more recently, hospital and university pharmacies.

METHODOLOGY: DISTRIBUTORS

A scammer will call a distributor directly "phishing" for account information by pretending to verify a pharmacy customer's licensure. They may pose as a vendor or try to impersonate State Boards of Pharmacy or other distributor employees, stating that they need account numbers so they can access correct invoices.

In certain instances, the scammers have used phrases such as, "there has been a glitch in the system," and they have asked a distributor's customer service representative to place the desired order themselves.

In some cases, where the scammer does offer an account number on their own, it has been found that the particular account does not have a previous history for the item they are requesting in an order — or that the account itself is old and has not been used for some time, or is closed.

Scammers also may try to create a new customer account, or change a customer's account information to their advantage by:

- Requesting to add additional names to an account;
- Changing or substituting different business addresses;
- Changing or substituting different account telephone numbers; or,
- Applying for a new line of credit.

THE DIVERSION ITSELF

Once the scammers have obtained pharmacy customer account credentials, they use that information to place what would appear to be a legitimate product order with the pharmacy's principal (or secondary) distributor. This can be done over the phone or online, as the scammer would, at that point, have the accurate identification information to place an order.

If the scammer is successful in creating the impression within the distributor's operations that a legitimate order has been placed by a pharmacy customer — and the distributor processes the order for shipment — the bad actors will then contact the pharmacy again, but now purport to be a distributor representative. In this conversation, the scammer will indicate that the pharmacy will be receiving a shipment that has been sent in error, or that a defective product has been shipped to them, that will need to be replaced.

The scammer will then tell the pharmacy representative that the distributor will be sending a courier to pick up the order to have it returned, reassuring the pharmacy customer that they will not be charged for the misshipment or will receive full credit for any defective product that requires a return.

The courier sent to make the pickup is not aware of the illicit activity, having simply received a routine request for a parcel pickup. The courier is most always an entity that the pharmacy customer has never used before.

The courier also ends up being scammed when they are contacted by the bad actor, again posing as a distributor representative, and told to deliver the return parcel(s) to a different address — typically that of a repackager, not the distribution center that originally shipped it.

The repackager is then scammed into sending the parcel(s) to a different location than that which was originally intended. That sequence of courier/repackager has been known to be repeated several times in a single shipment.

SCAMMER TECHNIQUES

Through **phone conversations** with distributor representatives, the scammers may appear overly confident, inpatient or even pushy — essentially acting more aggressively in attempting to get an order processed than what would typically be expected. In certain instances, the scammer may also attempt to convey a sense of urgency, which may lead the distributor representative to be sympathetic and let down their guard. In such an attempt, the scammer tries to appeal to the distributor representative's emotions by stating, "I really need this, as I'm out of supplies."

Visible telephone numbers in these communications between pharmacies and distributors (such as in a phone's "caller ID") are very frequently "spoofed" to appear as if they are being received from a legitimate entity.

Through **email communications**, the scammers similarly will "spoof" a legitimate email address by simply adding just a single letter or sequence of letters to the actual address itself. An example might be "sales@sampleaxinc.com," where an "inc" was added to what is the legitimate web address of "www.sampleax.com." The spoofed address still looks to be plausibly legitimate.

It is worth noting that in some of these email correspondences the scammers have used poor grammar, misspelled certain words or employed poor punctuation. In certain instances, the scammers inadvertently provide incorrect item numbers, omit National Drug Codes or can only spell the name of the product they are trying to order.

In all conversations/correspondences, the goal of the scammer is to gain control of the shipment without having to pay for it and then divert the parcel(s) to a different address. This may happen through direct communication to change the ship-to address or by a communication indicating the shipment is defective or was sent in error and needs to be returned — and ultimately through the medium of an unwitting courier.

These individuals are very adept at leading the person they are speaking with (whether a distributor representative or pharmacy customer) to fill in the gaps when engaging in transactional conversations. That "leading" technique subtly encourages the person they are talking with to:

1. Provide information that was not necessarily requested; or,
2. Correct certain information the scammer may have deliberately offered — in hopes that it would be clarified.

Historically, portions of this type of scam have been traced to several countries — including, but not limited to, Nigeria, Spain and Canada — but these scammers operate principally within the United States. The callers perpetuating the scam are often females. Names that have been used by the scammers in past successful interactions are "Sabrina Shaw," "Mary Wise," "Joanne Waterman," "Clancy Bidospech," "Kelly Jordan," "Rita Witt" — or simply a first name of "Allison", "Sasha" or "Susie."

Principal states where pharmacies are targeted have included Florida, California, Louisiana, Hawaii, New York, New Jersey, New Mexico, Georgia, South Carolina, Texas, Ohio, Wisconsin, Utah, Arkansas and Missouri.

RECOMMENDED ACTIONS TO PROTECT DISTRIBUTORS: RISK MITIGATION

There are several ways to validate correspondences with what appear to be legitimate distributor customers:

- Validate anything thought to be a suspicious email address: www.verifyemailaddress.org.
- Ensure any business phone number and/or address you are provided, in any type of account or credit modification/application matches a Yellow Pages "Reverse Lookup" (https://people.yellowpages.com/whitepages/phone-lookup). If the number in the yellow pages is different than the number on the credit app or account modification, call the number from www.yellowpages.com.
- Check the respective secretary of state office website for corroborating business information.
- Request a scanned or faxed copy of a specific business license, or driver's license to authenticate the request.
- Be wary of any customer using different customer names but the same address — or the same customer name but a different address.
- Be skeptical if the customer is willing to pay extra for overnight delivery but resides in a one-day delivery zone.
- Use Google Maps (www.google.com/maps) to verify any last-minute ship-to address changes.
- Consider the creation of a specific PIN for each customer, or a "security question," to strengthen the authentication process.

RECOMMENDED ACTIONS TO PROTECT PHARMACIES

Distributors can share specific actions every pharmacy should take to protect their business from this and other similar, damaging scams:

- If your pharmacy receives a suspicious call asking for account information or any type of distributor login credentials, the pharmacy representative taking the call should ask the caller for their name and phone number and simply hang up. Immediately after the call, the representative should report the details to their respective (known) distributor sales representative and request authentication. If the call is deemed suspicious the pharmacy should also notify their state's Board of Pharmacy.
- Protect your account information: login credentials, pharmacy license numbers, employee email addresses, etc., are privileged/private business information. All pharmacy personnel should be instructed not to share any of this information with anyone calling into the pharmacy. It is important to remember that a distributor will rarely, if ever, call you to request this type of private information.
- If a vendor calls the pharmacy, a pharmacy representative should call the vendor back directly, using distributor account information they already have or can reference.
- Take the time to verify all open orders with any distributor partners. If you do not see the order (in computerized tallies) that is being referenced in a call, then fraud is likely.
- If an individual purporting to be a representative of your distributor reports a defective product, call your distributor's customer support line for confirmation.
- Confirm wire payment requests with a known distributor representative before making any payment.

- Only release a return after you receive a proper, designated return authorization from your distributor partner. The only courier that should be permitted to pick up returns should be your pharmacy's regular contracted distributor driver. Call your distributor sales representative or the distributor's customer support line if a courier company, other than your regular courier driver/company, visits your site to pick up and process any return.
- Make sure your pharmacy staff is aware of these procedures so they are prepared to respond appropriately should a scammer call.
- Confirm wire payment requests with a known distributor representative before making any payment.
- Only release a return after you receive a proper, designated return authorization from your distributor partner. The only courier that should be permitted to pick up returns should be your pharmacy's regular, contracted distributor driver. Call your distributor sales representative or the distributor's customer support line if a courier company, other than your regular courier driver/company, visits your site to pick up and process any return.
- Make sure your pharmacy staff is aware of these procedures so they are prepared to respond appropriately should a scammer call.

WHAT YOU CAN DO TO ASSIST IN THESE INVESTIGATIONS

It is important in the investigation of these incidents that those pursuing criminal charges against the perpetrators know each and every time this has occurred (whether or not the attempt was successful). Helpful information would include:

- The date and time of the attempt(s).
- Whether the attempt made by phone or electronically.
- If the pharmacy — the store location as well as who within the store — spoke with the perpetrator(s).
- Any phone numbers or IP addresses that might have appeared during communications.
- The specific asks (language) used by the perpetrator.
- If contact was by phone, whether the caller was male or female.
- The name that the caller or emailer used.
- The information (if any) that may have been inadvertently provided to the perpetrator.
- Whether a voice recording of any phone conversation(s) exists with a perpetrator.
- The products discussed in any such order attempt.
- Whether any information was provided to a courier that would respond to pick up a misshipped order.

If your company has experienced a similar fraud incident or attempt, contact Chuck Forsaith of the PCSC at cforsaith@hda.org or (401) 623-1344. He can coordinate communications between your business and the appropriate law enforcement agencies. The Federal Bureau of Investigation and the U.S. Food and Drug Administration's Office of Criminal Investigations are jointly investigating these schemes, in coordination with the U.S. Attorney's Office.

The Healthcare Distribution Alliance (HDA) represents primary pharmaceutical distributors — the vital link between the nation's pharmaceutical manufacturers and pharmacies, hospitals, long-term care facilities, clinics and others nationwide. Since 1876, HDA has helped members navigate regulations and innovations to get the right medicines to the right patients at the right time, safely and efficiently. HDA's Pharmaceutical Cargo Security Coalition offers supply chain security intelligence; access to contacts from industry, government and vendor trade disciplines; physical and supply chain security assessments; a reference library of supply chain security publications, articles and related documents; as well as opportunities to attend educational events.

PCSC

HDA Pharmaceutical Cargo Security Coalition

901 North Glebe Road, Suite 1000
Arlington, VA 22203

(703) 787-0000
(703) 812-5282 (Fax)

www.hda.org/pcsc