Compliance Corner

Traci Morris, Compliance Coordinator

Please post in your respective area for anyone who makes purchases in your department – faculty, staff, and/or student workers. With a New Year brings new or revised scams, which on the surface appears to be a good deal. Be diligent when making purchases whether for your departments' behalf, or even a home purchase.

If it sounds too good to be true…

(U//FOUO) **SCAM TARGETING U.S. COLLEGES & UNIVERSITIES**

Handling Caveat:

In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees and contractors with a need to know. Exceptions to this rule may be authorized by the originating office or its successor in function.

(U//FOUO) The FBI is investigating an ongoing fraud scheme, likely originating in Nigeria, wherein unidentified subjects (Unsubs) purporting to be employees of U.S. universities fraudulently purchase items for resale or other unknown uses. Impersonated universities include a number of major universities throughout the country, with some receiving hundreds of notifications from defrauded companies.

While the merchandise ordered varies, the scheme generally follows the same pattern. First, the Unsubs set up a domain name which resembles the email address of an actual university. These domain names will generally have a .org or .com suffix rather than .edu. The Unsubs then contact retailers purporting to represent a university. The Unsubs request quotes for merchandise and send the retailer a credit application including legitimate information about the university they are fraudulently representing. Retailers are then sent fabricated purchase orders, with a “ship to” address that is different from the university’s actual address. The purchase orders typically incorporate the university logo, the correct billing address, and tax exempt documentation. The emails often include the name of an actual university employee; however, the telephone numbers and email addresses provided are controlled by the Unsubs.

The fraudulent purchase orders direct the merchandise to be sent to an address ostensibly associated with the university, often identified as an R&D facility. However, the addresses are generally for a shipping company, storage facility or residence. Storage units in multiple states have been established by the Unsubs in order to receive the merchandise. The Unsubs provide fabricated client information to these storage facilities and any fees are generally paid with stolen credit cards. The individuals receiving the merchandise often do so for a person they meet online, typically at a dating site or in response to a "work from home" advertisement. Once an order is placed, the Unsubs generally request tracking information for the packages to follow them to delivery. The Unsubs will contact the shipping company, individual, or storage facility receiving the goods to notify them when to expect the delivery. The Unsubs will subsequently provide them with directions for pick up by a third party carrier. Following pick up by the third party carrier, the packages are sent overseas, most often to Nigeria.

The items targeted by the Unsubs include a wide range of items. Fraudulently acquired items fall generally into two categories: electronics and laboratory/medical items. Electronics include hard drives, laptops, routers, cameras, video equipment, printer cartridges and supplies. Laboratory/medical items include bulk quantities of chemicals, multi-gas detectors, laboratory scales, magnetometers, centrifuges, incubators, and medical imaging equipment.

The universities whose identities have been co-opted have had some success getting the domain providers to repossess the bogus domain name established by the Unsubs. However, a new variation of their domain name is quickly established by the Unsubs after closing the original.

Investigations have been initiated and coordinated by several FBI field offices. In terms of financial fraud, the reported dollar loss for items shipped is in excess of $5 million. A number of shipments have been recovered.

Attempts to fraudulently use a university's identity as part of this scheme should be directed to your Campus Liaison representative with the FBI. Copies of the fabricated purchase orders and invoices generated should be obtained for the fraudulent orders and provided to the FBI. In cases where victim companies report the shipment of goods

within a day or two of shipment, the information should be passed to the FBI expeditiously in order to attempt to intercept and recover the goods.