(U) African Cyber Criminal Enterprise Members Using “School Impersonation” Scheme to Defraud Office Supply Retailers

(U) African Cyber Criminal Enterprise (ACCE) members, a posing as school officials, b are defrauding office supply retailers by purchasing large volumes of merchandise using fraudulently obtained lines of credit. While this scheme has reportedly affected only office supply retailers, recent successful attempts may lead ACCE members to use this scheme against other retail stores. This advisory will inform the reader how the scheme works, offers measures to help mitigate the threat, and advise how to report incidents to law enforcement.

(U) How the Scheme Works

(U) Step 1

(U) An ACCE member, posing as a school official, contacts a retailer's customer service call center by telephone or e-mail. Using social engineering tactics, c the ACCE member attempts to gather additional information on the school’s purchasing account. The ACCE member typically terminates the phone call or e-mail session once sufficient information is gathered to place an order. ACCE members also obtain account information from the school’s public Web site, if available.

(U) Step 2

(U) The ACCE member makes a second contact with the target store, this time representing himself as a school official and providing the account information obtained from step one. Billing to the school’s line of credit, the ACCE member makes large purchases of laptops, routers, hard drives, printer toner, and printer ink, with some orders totaling more than $200,000.

---

a (U) The term “African Cyber Criminal Enterprise” refers to individuals of African origin who commit various cyber-assisted fraud schemes and organize themselves in a loose network.

b (U) ACCE members have reportedly posed as officials from a range of educational institutions, including elementary, middle, and high schools; private and charter schools; and universities.

c (U) The term “social engineering” refers to the act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information.
(U) Step 3

(U) During the purchase, the ACCE member provides the customer service representative with a US shipping address, typically belonging to a victim of a "romance scam" or "work from home" fraud scheme. An ACCE member contacts the online scam victim and directs the individual to re-ship the office supplies to an address in West Africa, typically Nigeria, or to a US-based storage facility. To facilitate the re-shipment, the individual receives a shipping label prior to receiving the office supplies.

(U) In a more recent variation of the scheme, the ACCE member provides the true shipping address of the school they are purporting to represent. The ACCE member then contacts the school, posing as an employee of the office supply store, claiming that the products were shipped to the school in error. The school, believing it is returning the products to their rightful owner, reships the items to a domestic address provided by the ACCE member. Recruited individuals in the United States then re-ship the products to a West African country, commonly Nigeria.

(U) Once the fraudulent payment methods are discovered, retailers absorb the financial losses without charging the school system. See the graphic below for a depiction of a common variation of the school impersonation scheme.

---

\[d\] (U) An ACCE member, posing as an employer or romantic interest, gains the trust of individuals searching for employment opportunities or a romantic relationship. After a period of social engineering, the individuals are convinced to serve as money remitters or re-shippers on behalf of the ACCE members.
(U) Incidents in the United States

(U) Incidents of school impersonation fraud have affected schools and office supply retailers in California, Florida, Massachusetts, New York, Ohio, Pennsylvania, South Carolina, Texas, and Virginia. In most cases, the ACCE members telephonically contact the retailer to probe for information and place orders. Internet protocol (IP) addresses used by the ACCE members to place Internet orders typically are not masked by a proxy or virtual private network (VPN) servers. To date, approximately 95 percent of the school impersonation orders have been detected and stopped by office supply retailers.

- (U) Between July 2013 and early December 2013, suspected ACCE members, using the school impersonation scheme, defrauded a US-based office supply retailer of more than $270,000 with a total of $1.6 million in attempted losses. During the same time period, a second US-based office supply retailer was exposed to approximately $100,000 in losses stemming from the scheme.

(U) Mitigation to Counter School Impersonation Scheme

(U) Mitigation steps for consideration in countering a school impersonation scheme include:

- (U) **Customer Service Training:** Consider providing security awareness training to customer service employees to detect social engineering attempts against them.
- (U) **Protecting Purchasing Account Information:** Schools are encouraged to only post purchasing account information (i.e. usernames and passwords) on secure Web sites which are not available to the general public.

(U) Reporting the Crime

(U) The FBI encourages victims of a school impersonation fraud scheme to report it to their local FBI office [http://www.fbi.gov/contact/fo/fo.htm](http://www.fbi.gov/contact/fo/fo.htm). You will be asked to provide the following information:

- (U) Identifiers for the perpetrators, e.g., name, telephone number, e-mail address information;
- (U) Details on how, why, and when you believe you were defrauded;
- (U) Actual and attempted loss amounts;
- (U) Other relevant information you believe is necessary to support your complaint; and
- (U) Reference school impersonation scheme. If known, reference any ties to African countries.

---

(U) A virtual private network extends a private network across a public network(s), like the Internet, while maintaining functionality and security.