Federal Bureau of Investigation
May 2011

The FBI has developed information that banks and banking employees may be targeted by a fraud scheme conducted by an individual or group believed to be operating outside the United States.

Banking institutions and banking employees should be alerted to this potential scheme as it potentially targets personal employee information, customer information and banking security information.

Banking employees are being contacted by individuals who claim to be officials with the employee's bank headquarters or main branch location but who are, in reality, attempting to perpetrate a fraud. The individuals may use the name and other identifying information of a legitimate bank employee. Bank employees may be informed that they are the subject of a complaint that is being investigated. Voice mail messages may be left for a bank employee directing them to return the call to a telephone number with an 866 or 800 prefix. Employees are then asked to 'confirm' their employment status by either providing personal information (social security account number or other identifying number) or provide information relating to internal banking security (PIN's or authorization codes related to funds transfers).

Those perpetrating this fraud appear to be aggressive and well-organized. They may be using social engineering tactics in order to convince their victims they are legitimate employees. Social engineering is the gathering of information from multiple sources, including the bank's internet site, social networking sites, and through phone calls and emails. Frequently, these requests for information seem routine. Individuals using social engineering techniques can assemble small bits of information into a comprehensive organizational map or repeat procedures that may convince bank employees of the legitimacy of the identity of the person committing the fraud. Once the required information is gathered, the perpetrators of the fraud may attempt to contact the bank and execute wire transfers or other banking transactions for their benefit. When heard over the telephone, these individuals may have an accent indicative of origins in a foreign country.

Specifically, all banking employees should be reminded about the dangers of divulging personal identifying information about themselves or other employees and information regarding methods or validations of bank transactions or operations to individuals over the telephone or by email when the identity of the other person cannot be confirmed. Additionally, when returning calls of this nature, employees should independently confirm the name and telephone extension of an unfamiliar calling party.

Banks are encouraged to review security procedures in light of this information and implement procedures to protect the bank and the employees from potential loss due to this fraud scheme. Although some of the specific known tactics have been outlined, banks should be vigilant for variations as perpetrators of this type have been known to change their tactics if current schemes become unproductive.

Banks or bank employees that believe they have been the victim of this fraud scheme and have monetary losses should contact their local police department or FBI Field Office.