## Suspicious Activity Reports Document Transactions of International Fraud Ring

In a case that started when a bank notified federal agents that it intended to file a SAR on two subjects, investigators utilized BSA records to uncover additional participants in a fraud scheme. The investigation determined that the participants used stolen account information to steal funds and then wire the illicit proceeds to a foreign country.

A federal grand jury later indicted the two original subjects for their role in the fraud scheme. According to the indictment, the pair obtained account information stolen from financial institutions, created unauthorized access devices encoded with the stolen account information, and made unauthorized withdrawals from ATMs with the access devices. The indictment charges both defendants with conspiracy to commit wire fraud, wire fraud, and possession of device making equipment. One defendant was also charged with possession of unauthorized access devices with intent to defraud.

The indictment alleges a scheme to defraud whereby the defendants and a third co-conspirator received stolen financial institution account information from a fourth co-conspirator in a foreign country. The defendants then created unauthorized access devices encoded with the stolen account information and used these devices to make unauthorized withdrawals from the accounts via ATMs. After taking their portions of the proceeds, the defendants then wired the remaining funds to various individuals outside of the United States in amounts structured below the reporting requirements. The scheme resulted in discovered losses of more than $400,000.

According to the indictment, the pair and a co-conspirator initiated the conspiracy and the scheme to defraud. As part of the plan, a fourth co-conspirator periodically sent stolen financial account information, including account holder names, account numbers, passwords, and personal identification numbers via email. Once the defendants received the stolen account information, they programmed that data onto magnetic strip cards to create unauthorized access devices, which could be used in ATMs to make unauthorized cash withdrawals from the accounts. They used a laptop computer, and a manual magnetic card reader/writer to program the stolen information onto various magnetic strip cards, such as grocery store club cards and drugstore gift cards, to create the unauthorized access devices.

Eventually, the co-conspirator outside of the United States stopped sending stolen account information. At that point, one defendant returned to the foreign country to obtain stolen account information himself or recruit another individual to do so. The defendant eventually became the source of stolen account information, and the other two defendants shared their proceeds with him.

The case began when a bank identified the two initial subjects structuring cash deposits and subsequently wiring the funds out of the country. The bank also noticed that both subjects wired money to the same beneficiaries outside the United States. On the SAR,

the bank also noted that the accounts were personal accounts, which did not have payroll deposits or debits normally seen on personal accounts.

All three of the subjects committing crimes in the United States were additionally listed on money services business SARs. These SARs also focused on funds transfers, which appeared to be structured to avoid the $3,000 record-keeping requirement. Again, multiple structured wire transfers had the same beneficiary.

[Published in The SAR Activity Review – Trends, Tips & Issues, Issue 13, May 2008]