



Be Careful with Master Passwords for ATMs

*Issued by the Global ATM Security Alliance and the ATM Industry Association,
In association with Palm Desert National Bank
February 2005*

Actual Fraud Risk Scenario

In our continuing efforts to minimize risk exposure for our members, we are providing the following information about ATM master passwords. As we all understand, ATMs, in the vast majority of cases, are initially distributed from the factory with master passwords pre-set.

Recently, we have been advised of situations in which Master Passwords for ATMs have been compromised, either by not having these changed from the initial factory settings, or by allowing this information to be available to individuals other than the ISO/ATM deployer directly responsible for the installation. In these examples of fraud, unknown suspect(s) gained access through the master password and reprogrammed the cassettes to lower the cash dispensing denomination indicated *below* the required denomination, resulting in cash losses to the deployer¹.

Proposed Preventive Measure

To prevent this kind of compromise from happening, these master passwords should be changed at the time of site installation.

Information related to master passwords should never be divulged.

¹ In the USA, vault cash agreements normally place the burden for such loss with the ISO.