

AvoID Theft: Deter, Detect, Defend

The title of this article is the name of a new program announced recently by the **Federal Trade Commission** (FTC) designed to educate consumers and coincide with the creation of a task force designed to tackle this fast growing crime. According to FTC Chairwoman Deborah Platt Majoras, personal information is the new currency. She advises consumers to protect their personal information as carefully as they protect their cash.

The Identity Theft Task Force will be chaired by Attorney General Alberto R. Gonzales and co-chaired by Ms. Majoras and there will be representatives from 13 government agencies on the task force. According to the White House press briefing the task force's goal is to "make sure that this government of ours uses our assets in a responsible way, in a good way, to not only put those people who commit identity fraud in jail, but to help the victims of identity fraud."

The FTC is preparing education kits that will be sent to about 4,500 victim advocates across the country. It will include several brochures and a 10-minute video on identity theft. Until those kits and the task force's strategic plan are available, Ms. Majoras urged consumers to following safeguards, including *deter* (monitoring your personal information); *detect* (taking steps to reduce ID theft); and *defend* (acting quickly once identity theft is suspected).

Where do e-crimes occur?

With the emphasis being placed on ID theft and the number of reports the public hears about personal information being stolen, lost, sold, etc., one might think that the majority of e-crimes are committed by external hackers. However, a new survey commissioned by security firm Websense reveals that almost half of global e-crime experts believe the biggest threat to organizations' data comes from the enemy within.

Only 11 percent of the IT security professionals who were polled argued that external threats pose a bigger issue. The survey also revealed that only eight percent of those responding believed the "average" company takes a proactive approach to security while 59 percent reported that companies were only reactive.