# U.S. Department of Justice

# Operation Web Snare

A Joint Law Enforcement Initiative

OPERATION
WEB SNARE
DEPARTMENT OF JUSTICE - FEDERAL TRADE COMMISSION– U.S. POSTAL INSPECTION SERVICE - U.S. SECRET SERVICE
FEDERAL BUREAU OF INVESTIGATION – NW3C – IC3 – BUREAU OF IMMIGRATION & CUSTOMS ENFORCEMENT

August 26, 2004

# Web Snare

Executive Summary:

Operation Web Snare represents a coordinated initiative targeting an expansive array of Cyber Crime schemes victimizing individuals and industry worldwide. This initiative highlights numerous investigations that have been successfully advanced through cooperation and coordination of law enforcement, and a growing list of industry partners.

Cases included in Operation Web Snare exemplify the growing volume and character of Cyber crimes confronting law enforcement, and also underscores the continuing commitment of law enforcement to aggressively pursue Cyber criminals, both domestically and abroad. Focused efforts to pursue Cyber criminals internationally, has led to the development of enhanced proactive capabilities in several countries, and numerous investigative successes highlighted within this initiative. The development of international resources is closely coordinated with the DOJ, the U.S State Department and a growing list of E-Commerce industry partners.

Criminal schemes included in this initiative include: criminal spam, phishing, spoofed or hijacked accounts, international re-shipping schemes, Cyber-extortion, auction fraud, credit card fraud, Intellectual Property Rights (IPR), Computer Intrusions (hacking), economic espionage (Theft of Trade Secrets), International Money Laundering, Identity Theft, and a growing list of “traditional crimes” that continue to migrate on-line.

The substantial accomplishments captured in this initiative are attributable to the growing number of joint Cyber-crime task forces established across the U.S. Over the past year, more than 50 such task forces have either been established or significantly augmented with resources from numerous federal, state, and local agencies. Substantial industry partnerships developed in coordination with associations such as the Direct Marketing Association (DMA), the Merchants Risk Council (MRC), the Business Software Alliance (BSA), and the Software and Information Industry Association (SIIA) also contributed significantly to the success of this initiative. Operation Web Snare has been coordinated at the Federal level with the Department of Justice, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3), the U.S Postal Inspection Service, the U.S. Secret Service, the Federal Trade Commission, and the Bureau of Immigration and Customs Enforcement. Numerous state and local law enforcement agencies contributed significantly to this initiative as well. State and Local participation in this effort was amplified in coordination with The National White Collar Crime Center (NW3C).

Operation Web Snare includes more than 160 investigations, in which more than 150,000 victims lost more than $215 million dollars. Through these investigations more than 350 subjects were targeted, resulting in 150 arrests/convictions, 117 indictments, and the execution of more than 170 search/seizure warrants. Although significant in number, these investigations represent only a fraction of the Cyber crime problem, underscoring not only the need for sustained law enforcement focus, but the continuing development of expanded industry partnerships as well.