INITIATIVES

The IC3 participates in multiple initiatives targeting an array of cyber crime schemes that victimize individuals and businesses domestically and abroad. These initiatives are a coordination of industry resources along with the investigative resources provided by cyber crime task forces comprised of federal, state, and local law enforcement agencies. The success of these initiatives is directly attributable to the inclusion of the industry resources. Initiatives focus on the following:

Charitable Contributions Fraud

Counterfeit Check Fraud

Identity Theft Task Force

International Fraud

Investment Fraud

Online Pharmaceutical Fraud

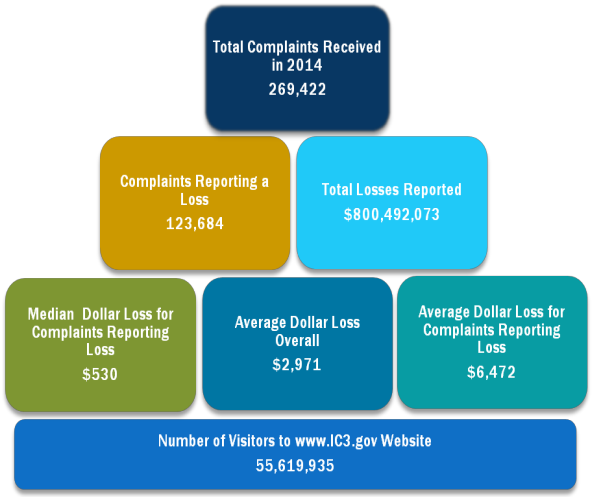
Phishing

Work-at-home scams

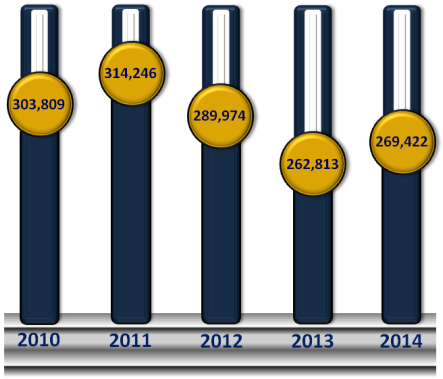
STATISTICS

2014 IC3 Statistics:

3,175,611
Complaints Reported to IC3 Since Inception



IC3 Complaints by Year



www.ic3.gov

AN INVESTIGATIVE LOOK INTO THE IC3

Mission of the IC3:

The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with industry partners. Information is processed for investigative and intelligence purposes for law enforcement and public awareness.

The IC3 Alliances:

The IC3 Unit is part of the Cyber Division's Cyber Operations Section V within the FBI. The IC3 Unit is staffed by FBI agents and professional staff employees with expertise in the prevention, detection, and investigation of cyber crime.

The IC3 has formed additional alliances with industry representatives (e.g. online retailers, financial institutions, Internet service providers, and parcel delivery providers) that have exponentially increased the flow of the IC3's most valuable commodity - INFORMATION. Working with federal, state, local, and international law enforcement, as well as regulatory agencies, IC3 analysts receive, develop, and subsequently refer information for investigative and prosecutive attention.

Cyber Crime and the IC3:

As technology evolves, so do the many methods used to exploit technology for criminal purposes. Nearly all crime that once was committed in person, by mail, or over the telephone can be committed over the Internet. The criminal element is empowered by the perceived anonymity of the Internet and the ease of access to potential victims. Criminals use social engineering to prey on their victims' sympathy, generosity, or vulnerability. The IC3 was designed to help address all types of cyber crime through its complaint system.

IC3 Complaints:

The complaints submitted to the IC3 cover an array of cyber crime including theft of intellectual property rights, computer intrusion, economic espionage, online extortion, and international money laundering. Numerous fraud schemes such as identity theft, phishing, spam, reshipping, auction fraud, payment fraud, counterfeit goods, romance scams, and non-delivery of goods are reported to the IC3.

Searching the IC3 Database:

The IC3 recently expanded the remote search capabilities of the IC3 database making it available to all sworn law enforcement and FBI personnel through the Law Enforcement Enterprise Portal (LEEP). Users can connect directly to the IC3 Complaint Search after authenticating through LEEP from the user's Identity Provider (IDP) or through the user's Law Enforcement Online membership at www.leo.gov. Users may also contact the IC3 for analytical assistance. While developing a case in the database, Management and Program Analysts compile similar complaints, collect relevant case information from both open-and-closed source public information databases and confer with federal, state, local and international law enforcement personnel. The IC3 complies this information into reports that are available to all law enforcement.

Public Service Announcements:

The IC3 prepares public service announcements on the latest cyber trends to alert consumers on Internet fraud. These announcements are posted on the following Web sites:

www.ic3.gov
www.fbi.gov