



UNITED STATES SECRET SERVICE ELECTRONIC CRIMES TASK FORCES

OVERVIEW

The United States Secret Service has gradually evolved since the agency's 1865 inception, from its initial mandate – suppressing the counterfeiting of U.S. currency – to protecting the integrity of the nation's financial payment systems. During this time, as methods of payment have evolved, so has the scope of the Secret Service's mission. Computers and other electronic devices are now the facilitators of criminal activity or the target of such, compelling the involvement of the Secret Service in combating cybercrime. The perpetrators involved in the exploitation of such technology range from traditional fraud artists to violent criminals – all of whom recognize new opportunities to expand and diversify their criminal portfolio.

To bring these perpetrators to justice, the Secret Service developed a new body, the Electronic Crimes Task Force (ECTF), to increase the resources, skills and vision by which state, local, and federal law enforcement agencies team with prosecutors, private industry and academia to fully maximize what each has to offer in an effort to combat criminal activity. The common purpose is the prevention, detection, mitigation, and aggressive investigation of attacks on the nation's financial and critical infrastructures. The agency's first ECTF, in New York, was formed based on this concept in 1995.

ECTF NETWORK

On October 26, 2001, President George W. Bush signed into law H.R. 3162, commonly known as the USA PATRIOT Act. The Secret Service was mandated by this law to establish a nationwide network of ECTFs in addition to the one already active in New York. These bodies collectively provide necessary support and resources to field investigations that meet any one of the following criteria: significant economic or community impact; participation of organized criminal groups involving multiple districts or transnational organizations; or use of schemes involving new technology. Investigations conducted by ECTFs include crimes such as computer generated counterfeit currency; bank fraud; virus and worm proliferation; access device fraud; telecommunications fraud; Internet threats; computer system intrusions and cyber-attacks; phishing/spoofing; assistance with Internet-related child pornography and exploitation; and identity theft.

Secret Service ECTFs are present in the following locations:

- Atlanta
- Baltimore
- Birmingham
- Boston
- Buffalo
- Charlotte
- Chicago
- Cleveland
- Columbia, SC
- Dallas
- Houston
- Kansas City
- Las Vegas
- Los Angeles
- Louisville
- Memphis
- Miami
- Minneapolis

UNITED STATES SECRET SERVICE ELECTRONIC CRIMES TASK FORCES

- New Orleans
- Phoenix
- Washington, DC
- New York/New Jersey
- Pittsburgh
- London
- Oklahoma
- San Francisco
- Rome
- Orlando
- Seattle
- Philadelphia
- St. Louis

FOR MORE INFORMATION

Please visit www.secretservice.gov/ectf.shtml for more information about Secret Service ECTFs. For more information about the Stop.Think.Connect.™ Campaign, please visit www.dhs.gov/stophinkconnect.

Stop.Think.Connect. is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit <http://www.dhs.gov/stophinkconnect>.



**Homeland
Security**

www.dhs.gov/stophinkconnect



STOP | THINK | CONNECT™