



4121 WILSON BOULEVARD, SUITE 101 • ARLINGTON, VIRGINIA 22203 • www.i-lawgroup.com • tel.703.243.8100 • fax.703.243.8162

About Us

Internet Law Group is a boutique law firm representing corporate victims of fraud committed over the Internet (phish, spam, malware, botnet operations, online sale of counterfeit and pirated products, online trademark infringement, etc.). Our practice is built on the premise that Internet fraud is a “common enemy” of our clients. In fighting this common enemy, our clients seek a common objective – to reduce the impact Internet fraud has on their business.

We help our clients achieve this objective by collecting information about acts of Internet fraud from across our client base and other sources, using automated systems developed in-house. We trace the acts back to their human source, using a variety of formal and informal information-gathering techniques. Our clients hire us to increase the intelligence of their own work, and to expand their view into the world of cyber-fraud. Because of the efficiencies in our practice, most of our work is performed under a cost-effective fixed monthly retainer, with hourly rates applying to advanced work targeting specific fraudsters. Our clients also appreciate and benefit from the strong privileges and protections that flow from our role as private sector lawyers directly representing private sector clients. Leveraging off all that we know, we work with our clients to develop and implement effective offensive actions (civil litigation as well as criminal referrals) that target the major fraudsters victimizing our clients.

In a nutshell, our clients understand we know how to identify fraudsters and understand they each benefit from appropriately restricted sharing of information about their common enemy, about themselves, and about their roles as victims of Internet fraud.

What We Do For Our Clients

eFraud Reporting Center: We receive real-time electronic reports from clients, the general public and third-party private sources regarding fraudulent websites. Our reporting sources include ISPs and ESPs, honey pot and honey net email, as well as public and private reporting systems.

Automated eFraud Investigator: Our eFraud Reporting Center deploys automated eFraud “investigators” in real-time to collect critical, short-lived information regarding fraudulent websites reported to the Center. These investigators capture the vital evidence we need to identify both the fraudster and those providing enabling services to the fraudster. This data capture is the first wave in our broad offensive against fraudsters.

eFraud Analysis & Cluster Reporting: Using the evidence collected by our eFraud Investigators, we analyze fraudulent websites and those enabling them and periodically report to our clients on patterns and trends. We also identify hot spot clusters that are enabling more than their fair share of fraud. These hot spot clusters are often compromised networks or negligent providers who are being abused by their failure or inability to adopt best practices. Increasingly, however, the clusters represent co-conspirators who provide “cover” to fraudsters in exchange for a portion of the illicit gains. We can also make available to our clients and their anti-fraud teams the information we acquire through our Reporting Center and eFraud Investigators.

“PIER” Legal Notices: Based on our trend analysis, our law firm issues formal legal notices to hot spot cluster owners and others enabling the fraud. These legal notices serve two key purposes: First, they leverage our clients’ own anti-fraud resources by putting white hat enablers on notice of their role in the fraud, and provide white hats with concrete information and advice on how to take action to correct their problem and share information with us about the fraudster, through **P**reservation of information, **I**nvestigation, **E**nforcement of their own policies, and **R**eporting to us on the result of their own investigation and the identity of the fraudster. Second, PIER Legal Notices identify and isolate black hat enablers who fail to respond appropriately to our legal notices.

Formal Information Collection: Hot spot clusters that fail to respond to our legal notices are targeted for increasingly substantial investigative and legal actions. For example, we deploy private investigators to initiate undercover purchases from fraudulent websites or to salt a fraudster’s phishing database. We also file civil lawsuits against “John Doe” fraudsters to obtain subpoena power over enablers who are unable or unwilling to cooperate informally.

Formal Enforcement Actions: Armed with all that we can know about a fraudster, we strategize with our clients to develop an enforcement action plan. The options extend far beyond simply filing a civil complaint against the fraudster. For example, a fraudster’s assets can sometimes be frozen under trademark law. Alternatively, enablers can be subject to civil liability for conspiring with fraudsters. We also work closely with private sector Internet security firms and domestic and international criminal law enforcement and other government agencies to formulate solutions to acts of Internet fraud, including those that threaten national security and critical infrastructure.