



FOR IMMEDIATE RELEASE – Thursday, September 18, 2014

Contact: Adam Benson, 202.999.9104, [adam@digitalcitizensalliance.org](mailto:adam@digitalcitizensalliance.org)

# Taking Credit: How to Get Away With Stealing \$96 Million Dollars Worth of Movies and TV Shows

*New Report Shows Credit Cards Make It All Too Easy for Rogue Cyberlocker Operators To Make a Fortune on Other People's Work*

Washington, DC – Stealing movies and television shows has become a multimillion-dollar industry with rogue cyberlocker operators generating considerable revenues and enormous profit, according to a new report today by NetNames. Just as troubling is the finding that some of America's best known and respected credit card companies are making it all too easy for these cyberlockers to sell the stolen works of content creators.

[“Behind the Cyberlocker Door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions.”](#) a NetNames report commissioned by online safety group the Digital Citizens Alliance, shows that 30 leading cyberlockers make a combined \$96.2 million dollars a year

“We’ve never had a business dependent on criminal activity grow and thrive in plain sight like the content theft industry,” said Digital Citizens Alliance Executive Director Tom Galvin. “It’s astounding to think of 30 sites making \$100 million dollars on products they’ve stolen from content creators. We’re just as troubled by what NetNames found from actually looking at the sites: cyberlockers wouldn’t thrive, perhaps not even survive, without legitimate businesses facilitating the rogue operators’ activities.”

NetNames found that of the twenty-five sites that offered a premium subscription, all but one accepted credit cards. This is a critical component of the cyberlockers’

business models – as 54.3 percent of the sites revenues come from customers who purchase premium subscriptions.

“Content theft fuels the success of cyberlockers and the facilitators of this business model - like payment processors and the advertising industry – frequently do nothing to prevent their successful operation,” said David Price, Head of Piracy Analysis at NetNames. “Without the subscription payments, revenues and profit – particularly for the direct download cyberlockers – would drop off dramatically. Remove the payment processors from the equation and it becomes far more difficult for cyberlockers to profit from the work of others.”

The actions of PayPal could serve as an example: three years ago, PayPal was the payment method of choice for rogue sites like cyberlockers. In 2014, NetNames found that only a single cyberlocker accepted premium subscriptions through PayPal. “Many rogue sites do not even contemplate using PayPal to gather revenue anymore,” Price observed. “PayPal’s refusal to do business with cyberlockers demonstrates that it is possible to monitor and control the use of payment systems.”

Congressman Adam Schiff (D-CA), Co-Chair of the International Creativity and Theft-Prevention Caucus, commended this new research, saying: “For several years, I have been working with my co-chairs on the International Creativity and Theft-Prevention Caucus, which I’m proud to co-chair, to champion a ‘follow the money’ approach which encourages voluntary measures by responsible actors in the online ecosystem to cut off profits to sites engaged in piracy. The report today adds important new details and data to that effort, making clear that certain unscrupulous cyberlockers are realizing millions in profits through a business model that turns a blind eye, or even encourages, large scale piracy. It’s incumbent on payment processors, advertising networks, and other online services to take voluntary steps to reduce the profits realized through massive theft of U.S. content.

#### A Deeper Dive into the NetNames Numbers:

NetNames analyzed the fifteen most popular direct download cyberlockers (which store files for users to download to their computers) and the fifteen most popular streaming cyberlockers (which host video files that users stream, rather than download).

- Direct Download Cyberlockers

- The 15 largest direct download cyberlockers combined to make \$63.1 million in annual revenue (\$4.2 million per site in annual revenue). Direct download cyberlockers averaged \$2.7m profit each, from revenue of \$4.2m, a rate of profit of 63.4 percent.
- 70.6 percent of direct download cyberlocker revenue came from subscription services enabled by payment processors, and 29.4 percent came from advertising.
- Streaming Cyberlockers
  - The 15 largest streaming cyberlockers combined to make \$33 million in annual revenue (\$2.2 million per site annually). These sites averaged \$1.9 million in profit – a rate of profit of 87.6 percent.
  - 71.1 percent of streaming cyberlocker revenue came from advertising and 23.1 percent from premium account subscriptions enabled by payment processors.

“A small number of advertising networks are willing to deal with rogue sites,” Price said. “But they are able to locate enough advertising – sometimes from premium brands – to make these sites not just operational but wildly profitable.”

- The overwhelming use of cyberlockers is for content theft. At least 78.6 percent of files on direct download cyberlockers and 83.7 percent of files on streaming cyberlockers is copyrighted content – stolen and sold illegally.

Galvin added: “There is only one way to explain these enormous profit margins: These operators don’t make anything. What they sell is stolen content. You can make a lot of money taking the works of others and selling them on the Internet. And that very activity erodes confidence in the Internet by harming brands, confusing consumers and potentially turning respected companies into accomplices.”

This is the second report commissioned by Digital Citizens Alliance demonstrating that content theft is not a cottage industry. Previously, in the “Good Money Gone Bad” report this activity makes hundreds of millions of dollars for the operators. Key findings from that report include:

- The largest 596 ad-supported content theft sites reaped nearly a quarter of a billion dollars (\$227 million) in ad revenue in 2013.
- 30% of the most heavily trafficked content theft sites carried premium brand advertising. Those are the blue chip, highly recognizable brands.

## **About the Digital Citizens Alliance**

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet and the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place. Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical and creative industries as well as online safety experts and other communities focused on Internet safety. While all Digital Citizens hold themselves personally responsible to do all they can to protect themselves and their families, we are also concerned that technologies, standards, and practices are in place that will help keep all of us safe as a community. Industry has a critical role to play in ensuring those safeguards are established and updated as needed to address the continually evolving challenges we face online. Visit us at [digitalcitizensalliance.org](http://digitalcitizensalliance.org).

## **About NetNames**

NetNames provides companies with global reach on the Internet whilst protecting their brands from online fraud. As the global leader in this field, NetNames has been chosen by many of the world's most successful brands to enable and protect their internet presence. With online channels becoming increasingly important for a corporate's commercial and marketing activities, NetNames offers a single point of contact for management of domain names, in all locations, globally, and protection for brands across all online environments. NetNames offers expertise, infrastructure and service levels that are hard for corporates to replicate internally and enjoys long term relationships with large and mid-sized corporates. Headquartered in London, NetNames' global network includes offices in Cambridge, Paris, Copenhagen, Stockholm, Zurich, Munich, New York, San Francisco, Melbourne and Singapore.