

## WIRELESS INDUSTRY FIGHTS BACK AGAINST PREPAID PHONE TRAFFICKING

Cell phone trafficking operations siphon millions of dollars from the wireless industry and its customers every year. Until recently, little could be done to fight back, but a vigorous counter-attack, that has yielded several victories in federal courts across the country, is beginning to turn the tide and help the wireless industry put a stop to a spreading epidemic.

### **How the Scam Works**

Cell phone traffickers have created a complex network of individuals and companies in the U.S. and around the world that steal subsidies from wireless companies used to lower the cost of their phones for legitimate customers. Traffickers divert subsidized phones by hacking into their proprietary software, and then resell the phones at a substantial profit in the US and in other countries where they can be used on other wireless networks. Ultimately, the losses from this theft are passed along to American consumers and businesses in the form of higher prices for wireless phones and service. Although there is no industry-wide data on precise loss figures, based on investigations and litigation it appears that traffickers divert several million handsets from various wireless providers in the United States each year.

Although there does not appear to be a single entity orchestrating all of the worldwide trafficking, the networks of traffickers identified thus far appear to share common structural elements. The schemes involve groups of "runners" who purchase prepaid mobile phones at deep discounts from major retail outlets. Their "full time job" is traveling from store to store, buying the maximum allowable number of phones and then moving on to the next store.

Runners quickly resell the phones they buy to "middlemen" or resellers who remove the phones from their original packaging and prepare them for resale. First, the phones' proprietary software is hacked in order to allow the phones to operate on a network other than the one for which they were intended. Often, this process occurs in foreign countries with cheap labor prices and lax enforcement of intellectual property laws. Then, the hacked or "unlocked" phones are repackaged or "re-kitted" for resale.

The "re-kitting" process involves placement of the phones in new - often counterfeit - packaging along with a charger that operates on the target country's electrical system, counterfeit batteries, instruction manuals, warranties and other materials, all of which is intended to deceive the consumer into believing they are buying a brand new phone. The unsuspecting consumer who ultimately buys the phone here in the U.S., or in Ecuador or Malaysia, likely has no idea that their phone was originally sold at a Wal-Mart or Target store in Dallas or Los Angeles.

---

## **The Real Victims**

In addition to lost subsidy investment suffered by the American phone service providers and their legitimate consumers who are harmed by the losses that are ultimately passed along to them in the form of higher rates, the consumers who buy the hacked phones are deceived into buying inferior products. The phones were not designed or manufactured for use on their local networks, and the hackers often damage the phones' software as they stumble through the process of trying to unlock and reprogram the handsets to work on other carriers' networks. The counterfeit warranties are generally not valid, and the manufacturers either absorb the cost of fixing the damage caused by the hacker or refuse to fix phones that do not work properly because of the tampering. Consumers in this country also suffer because traffickers often buy up all the prepaid wireless phones in a store, leaving none for legitimate customers to buy.

## **Fighting Back**

TracFone Wireless, which has been a frequent target for phone traffickers, is taking action to stop the theft.

Starting in 2006, TracFone began an aggressive campaign of investigating runners, middlemen, unlockers and others involved in phone trafficking, and began filing lawsuits. Since that time, TracFone has filed more than 40 cases against nearly 150 separate defendants in federal courts in seven different federal district courts in Texas, Georgia, California, Florida, Michigan and New York. TracFone's lawsuits have so far resulted in more than 20 stipulated permanent injunctions and final judgments finding the traffickers' conduct illegal and prohibiting them from ever again buying, selling, unlocking or transshipping TracFone and Net10 wireless phones. TracFone has also been awarded millions of dollars in damages.

Other major wireless service providers have also taken aggressive action to shut down trafficking. AT&T, T-Mobile, IDT and Virgin Mobile have all filed similar lawsuits and are succeeding in getting courts to enter injunctions and award damages. In addition, wireless handset manufacturers Nokia and Motorola have also filed lawsuits against traffickers, focusing on their use of counterfeit packaging and components.

All of the wireless providers are constantly looking out for additional targets for litigation, and many more lawsuits will be filed in the coming weeks and months. The industry wants the perpetrators to know that they are all being pursued.

## **Uncharted Territory**

The industry also is working closely with law enforcement authorities to pursue and prosecute traffickers. The first trafficker to plead guilty to a crime associated with prepaid wireless phone trafficking is scheduled to be sentenced on August 22 in Houston, Texas. In May, Muhammad "Mubi" Mubishir plead guilty to criminal contempt of court before Judge Melinda Harmon of the Southern District of Texas for violating the court's injunction prohibiting him from trafficking in prepaid mobile phones. In deposition testimony and documents produced to TracFone, Mubishir

---

admitted trafficking more than 9,000 TracFone wireless phones, resulting in a loss of more than \$1.4 million to the company. Judge Harmon is expected to sentence Mubishir to prison time and require payment of restitution to the affected wireless companies. The Mubishir conviction represents an important milestone in the pursuit of phone traffickers, and additional criminal prosecutions are expected to be forthcoming in various parts of the country.

By James B. Baldinger  
Shareholder, Carlton Fields PA  
Counsel for TracFone Wireless, Inc.

*About the author:*

*James B. Baldinger is an attorney and a shareholder in the law firm of Carlton Fields, PA, and represents many telecommunications companies in litigation throughout the country. He previously served as Vice President of Business Security for AT&T Wireless Services, Inc. TracFone has set up an online tip service and a toll-free phone line to report suspicious activity. If you know anyone engaged in prepaid phone trafficking, if anyone solicits you to become involved in trafficking, if anyone tries to get you to become a runner or if you see anything suspicious, please contact the TracFone anytime, 24 hours a day, 7 days a week at (866) 806-1838 or [tracfone.security@tracfone.com](mailto:tracfone.security@tracfone.com).*

Re-printed with permission from E-Commerce Times, July 21, 2008, E-Commerce Times

---