

## GOING PHISHING – INTERNATIONAL

### Global Ring Gets Rather Slick

Federal Bureau of Investigation - 05/20/2008



They had quite a gig going, until a coalition of feds and foreign partners busted it up.

In a pair of related cases announced on Monday, a total of 38 people with links to global organized crime—mostly working out of Romania and the U.S., but also operating in Pakistan, Portugal, and Canada—were indicted for engineering a decidedly 21st century cyber-based scheme.

**It was rooted in what has become a fairly routine online crime:** “phishing,” a form of cyber seduction where you get an e-mail that looks like it’s from your bank or another trusted institution but

is really a way to con you into giving up personal information (PINs, social security numbers, credit card information, etc.)...along with its up-and-coming second cousin, “smishing,” which carries on the same ruse via text messaging.

**But what these criminals allegedly did—at least in the case based in Los Angeles—took this scheme a few steps farther**, giving the online scam a clever offline payoff and ultimately swindling thousands of people and hundreds of financial institutions out of millions before being shut down.

#### Here’s how it generally worked:

- Fraudsters working primarily out of Romania—known as the “suppliers”—went phishing and obtained thousands of credit and debit card accounts and related personal information by sending out masses of spam.
- These suppliers then sent their ill-gotten financial data to their partners in the U.S.—so-called “cashiers”—through Internet chat and e-mail messages.
- By using some sophisticated but readily available software and technologies, the cashiers manufactured their own credit, debit, and gift cards encoded with the stolen information, giving them unfettered access to large amounts of money via ATMs and point-of-sale terminals.
- Before these cards were used, cashiers directed “runners” to test the cards by checking balances or withdrawing small amounts of money from ATMs. Then, these “cashable” cards were used on the most lucrative accounts.
- To bring the scheme full circle, the cashiers wired a percentage of the illegal proceeds back to the suppliers.

**The L.A. investigation—as well as the second case based in Connecticut—was made possible through our growing partnerships.** In California, we worked with the U.S. Postal Service, the IRS, several local law enforcement agencies, and the Romanian General Inspectorate of Police. In the Connecticut case, our efforts dovetailed with the multi-agency Connecticut Computer Crimes Task Force.

The indictments, fittingly, come on the heels of a [comprehensive new strategy](#) to fight global organized crime by uniting the efforts of the Department of Justice and nine federal law enforcement agencies.

**The cases are a cautionary tale, of course, for anyone who uses e-mail or text messaging—which is most of us these days.** We can’t say it often enough: **don’t** respond to unsolicited e-mails or text messages from companies you do business with. If you aren’t sure, contact the company to verify that the message is legit.