



ISSUE #22 – 4<sup>th</sup> Quarter 2007

## Cell Phone Fraud – Part II of II

### Safeguard Personal Information

Based on Part I of our Cell Phone Fraud Newsletter, you know that you may be held responsible for fraudulent charges on a lost or stolen cell phone, but how else can you protect yourself from cell phone fraud? One way is to safeguard your personal information. Don't store information such as social security numbers, bank accounts, or work related data in your phone in case it is lost, stolen, or you turn it in for an upgrade.

Wireless and Bluetooth capabilities can make you vulnerable to certain security risks. Turn these services off if you don't plan on using them. A new form of cell phone fraud involves text messages. It begins when you receive an unwanted text saying a fake service has been purchased and that you must follow a link to unsubscribe to that service. This "mobile" phishing is similar to phishing emails online that have you giving away personal information on your computer. Once you follow the link on your cell phone, you may be instructed to download software that makes it possible for thieves to steal personal information from your phone. You can either turn off the text messaging feature if you will not be using it or just follow the same rule to avoid typical phishing scams: do not open or reply to messages that are sent from someone you do not recognize.

Cell phone worms are another potential security threat. Experts predict cell phone worms will infect at least 100,000 phones in 2007, jumping from phone to phone over wireless data networks. The good news, says one security consultant is that "cell phones have plenty of different operating systems, and for that reason, they're much harder to attack on a large scale."

### Delete your personal information correctly

Personal information on your cell phone can be resurrected. Moreover, deleting information on your cell phone is not always a simple process. Resetting your phone data does not ensure that earlier data has been permanently erased. Even though data may appear to have vanished, identity thieves can find ways to recover private information with special software.

Phone manufacturers usually provide detailed information on how you can completely delete personal information on your device. If you have questions or experience difficulty doing this, you may even want to take your phone to your carrier's

local office and have them permanently delete the information for you. The cost of having this done is money well spent, though one expert offers this foolproof recommendation: after purchasing your new phone, destroy the old phone just to be safe.

### Cell Phone Records for Sale

Another area of potential concern is the growing industry of phone records illegally bought and sold on the black market. Criminals can use your phone bill records. Your billing statement can reveal all matters of data that leave you open to identity fraud. So keep them in a safe place. Think of them as if they are your bank statements. You wouldn't carelessly toss them in the garbage?

The only place where telephone call records are legally kept is the phone companies. However, this doesn't prevent unauthorized people from seeking to get their customers' call records and sell them.

According to the Washington Post, "there are probably 100 such sites that offer to {illegally} sell phone records." Experts say data brokers and private investigators who offer cell phone records for sale probably get them using one of two techniques.

The first method for someone seeking call data is to try to get access to consumer accounts online.

The second is "pretexting," in which the data broker or private investigator pretends to be the cell-phone account holder and persuades the carrier to release the information. Having access to a Social Security number makes it easier to persuade a customer representative that the caller is indeed the account holder.

While federal law prohibits pretexting for financial data -- which at one time was a primary means of stealing credit card and other account information -- it does not cover telephone records, which are covered by a patchwork of state and federal laws governing access to personal information.

If you think you are a victim of pretexting, or any other type of identity theft, please contact Identity Fraud, Inc. at:

**1-866-4ID-FRAUD**  
(866-443-3728)