The Wall Street Journal Interactive Edition -- September 11, 1997

Stop, Thief!

AT&T's Roseanna DeMaria leads the effort to combat cellular-phone fraud

By WILLIAM M. BULKELEY

Last fall, AT&T Corp. scored a big hit in its efforts to keep people from ripping off cellular-phone numbers and putting them in new phones: The telecom giant helped police in Jacksonville, Fla., capture 61 drug dealers, pimps and a naval saboteur.

The sting operation was part of an unorthodox and increasingly successful campaign by AT&T Wireless Services to combat the epidemic of cellular fraud that in recent years threatened to slash industry profitability.

The campaign, which has given previously reluctant police a reason to care about cellular fraud, has been orchestrated by Roseanna **DeMaria**, a diminutive 40-year-old lawyer. AT&T recruited her in 1994 from her job heading narcotics prosecutions for the New York City district attorney's office.

Nancy Januzzi

Reseanna DeMaria

When Ms. **DeMaria** joined AT&T, cellular cloning was a serious threat to the fast-growing industry. Cellular bandits with electronic scanners could easily monitor the airwaves and capture the electronic code numbers that identified phones for usage and billing purposes. Then they would program the numbers into another cellular phone and sell it. Such cell-phone "clones" are illegal, but prosecutions were rare, because most DAs had better things to do: busting murderers, rapists and drug dealers.

Ms. **DeMaria** had a different view of cellular fraud, driven home by her time in the DA's office. She saw the number-snatching as a crucial tool of organized crime and especially the Colombian drug cartels, whose dealers and couriers needed go-everywhere electronic communications that couldn't be traced to them. When she interviewed for the job at AT&T Wireless's Kirkland, Wash., headquarters, she found herself in a sharp argument with her future bosses.

"I said, 'You're all confused if you think these criminals are in this for free service,' " she says. " 'The large-scale criminal enterprises are using it for

anonymity.' "

'Thinking Like a Dirtbag'

Cloning can be costly for cellular companies, even though legitimate phone owners never have to pay for such calls, and much of the fraud is simply unbilled use of airwaves. The cellular companies often have to write checks to each other for air time when a clone-phone is used as a "roamer" in another company's territory. The industry estimates total losses at $710 million last year, up from $650 million in 1994. Moreover, fraud can make people feel less secure about cell phones -- and therefore less likely to use them.

Theft in the Air

The cellular industry's losses to fraud

Year	Total Revenue (billions)	Losses to Fraud (millions)	Losses as % of Revenue
1996	$23.5	$710	3.0%
1995	17.1	650	3.8
1994	13.0	482	3.7
1993	10.9	365	3.4
1992	7.8	200	2.6
1991	5.7	100	1.8

Source: Cellular Telecommunications Industry Association

After taking the AT&T job, Ms. **DeMaria** has gotten prosecutors to take more interest in cellular theft by showing them that detecting it can lead to busts of hard-core criminals in narcotics and organized crime. By installing new technology, lobbying states to rewrite laws and providing training of cops and prosecutors, Ms. **DeMaria** has spurred an industry-wide reversal of the flood of cloning that threatened to undercut the entire business.

"I'm successful because I'm good at thinking like a dirtbag," says Ms. **DeMaria**. "I'm going mano a mano with the criminal, and AT&T Wireless is winning."

After being lobbied by Ms. **DeMaria**, Utah Senate Democratic leader Scott Howell rewrote the state's cellular fraud laws last year to make possession of cellular-phone knockoff equipment a felony. "I'd hate to go up against her in court," says Sen. Howell. "She's a lady who could rip your eyeballs out without blinking an eye."

Though fraud is still rising in dollar terms, all the lobbying has had an effect. As a percentage of industry revenue, fraud has declined to 3% from 3.8% two years ago, reversing years of increases, according to the Cellular Telecommunications Industry Association, a trade group. "We feel we're making real progress on classic cloning," says a spokesman.

AT&T Wireless, which has led the way in implementing sophisticated authentication, is doing even better at cutting down fraud. Ms. **DeMaria** won't disclose details, but she says cellular fraud is "well under" the 2% mark. She adds, "As an industry, we turned the corner last year."

To Catch a Thief

A big reason for the gains, along with enforcement efforts, was improvements in technology. These come in two flavors: those that are part of the phone, and those used by the service provider to detect suspicious use.

Once cellular companies decided cloners were a serious problem, many started requiring customers to use four-digit personal-identification numbers every time they started to use their phones. Because the PIN isn't broadcast except at the beginning of the call, it's hard for cloners to intercept. (The rest of the code number is continuously aired during the call.)

But many customers dislike tapping four extra keys. So, many cell companies are using RF analysis, in which the cellular provider checks to make sure that the radio-frequency emissions -- a sort of signature -- match the RF of the phone for which the code numbers were sold. The user doesn't have to do anything to be protected. A cloned number from a Motorola phone won't work in a Nokia, for example, Ms. **DeMaria** says. Many cellular services in big cities that have been plagued by cloning use RF analysis. One big drawback: It doesn't work when a user "roams" from one territory to another.

The level of security after that: authentication, which involves changing code numbers in digital phones. The technology involves each phone producing a unique number when queried by the central switch every few minutes that it's operating. If the phone produces the wrong number, the call is terminated. "Authentication is the Sherman tank," says Ms. **DeMaria**. "It will render the current cloner a dinosaur."

The operative word in that declaration is "will." Authentication works only with cellular phones that encode sound into digitized computer signals, which are just now being rolled out; it doesn't apply to the installed base of 50 million cellular phones that send sound in the traditional analog way.

Cellular companies also started analyzing customer use by computer to detect sudden changes in calling patterns that might indicate cloning. Two

years ago, the same clone number could be sold to dozens of different users around the country and the system wouldn't notice even if several used it simultaneously. Today, the system will not only notice immediately, but also attempt to figure out which is the legitimate user by seeing whether one is calling phone numbers it has called before and then shutting off the others.

Cellular companies have also taken other steps to hold down losses. When new customers get a phone, the company watches to see whether their usage pattern matches the usage they sign up for. For example, a customer who bought a basic $20-a-month package with very few free minutes but who is using the phone constantly looks like someone whose phone has been stolen or someone who doesn't plan to pay the phone bill.

All these steps mean that AT&T can identify and shut off clone phones much more quickly. "Clone phones used to have a shelf life of 45 days -- they were even sold with 30-day guarantees," says Ms. **DeMaria**. "Our longest period of time now is three days."

Nasty Warnings

After joining AT&T, Ms. **DeMaria** conducted focus groups of customers and found that many were aware of cloning and angry about it. So, while the industry used to play down the clone-phone problem, Ms. **DeMaria** raised its visibility. Last year, AT&T Wireless launched an advertising campaign on New York subways, ferries and buses. Showing a picture of a man holding a phone at a busy intersection, the ad read: "Cellular service has gotten very sophisticated. Now it can track the criminals who steal it."

At the same time, AT&T added a message to cloners in its customer-service messages when the fraud-management software detected a customer had been cloned. To the polite message sent to customers -- "Please hold on for a customer-service representative. We think you may have been a victim of cellular-phone fraud" -- AT&T added another for the thieves: "Please hold on while we analyze your location for referral to the proper authorities."

In reality, analysis of cellular-phone signals gives only an approximate location of a caller, and police aren't sent out to scour the streets for illegal phone users. But Ms. **DeMaria** says that such messages rapidly made people less eager to buy clones. "We want the users to know they aren't just being paranoid," she says. "We really are shooting at them."

Ms. **DeMaria** got an early taste of cellular technology in New York when she wanted to wiretap a criminal with a cellular phone. Such taps occur at a central switch, but unlike wiretapping a line telephone, which always goes through the same switch, wireless taps require identifying and tapping whatever switch is handling the particular call.

Ms. **DeMaria** said the hardest task was persuading the judge to let her tap

switches in neighboring New Jersey when the criminal was on the road.

"I had to learn the technology to explain probable cause to the judge," she says. But she realized that people using a cloned phone "showed criminal intent," a key to getting a tap approved.

Getting Cops' Attention

At AT&T, she applied that insight to getting cooperation from police. Her first few months on the job, she wrote a model statute, like the one adopted in Utah, that turned possession of cloning equipment into a felony and made use of a cloned phone in a crime a felony, similar to using a gun. Working with AT&T lobbyists, she helped get the felony laws passed in 18 states and the United Kingdom. The next step was teaching police that these laws could help them make cases.

AT&T teaches some 500 law-enforcement officials a month how to take advantage of the laws to track and nail criminals. It designed posters describing cellular fraud and how to identify equipment, and it will have distributed 21,000 of them by the end of this year. AT&T provided articles such as "Entering the World of Cellular Fraud," for police publications like the New York City Police Department's "Spin 3100" internal magazine. It made training videos demonstrating how prosecuting cellular crime could help in other cases.

"For law enforcement, this will never be a priority," she says. "We said, put this in your investigative arsenal."

This spring, AT&T helped Sacramento police bust two small drug rings. AT&T had detected a pattern of clone-phone usage. Under a law that permits it to listen in to protect the company from theft of services, Ms. DeMaria's investigators heard people on one set of clone phones talking over plans to fly to Los Angeles to pick up a package. AT&T turned the tapes over to police, who seized both drugs and cloning paraphernalia, pleasing both Ms. **DeMaria** and the police. "We give them the whole package," she says. "The police understand they'll get a quality product from us."

Her biggest success came in Jacksonville, Fla., last fall. After one of AT&T's monthly Fraud Fairs for police, officials approached AT&T and suggested establishing a front operation in which undercover cops would sell what were supposed to be clone phones if AT&T would provide free air time and keep track of the calls.

At its storefront, the police captured on video an array of drug dealers, prostitutes, escort-service operators and even a Navy man who was calling in bomb threats to the base.

Ms. **DeMaria** thinks such stings are paying off big for the industry. "Next time someone buys a clone phone, they have to ask, 'Am I buying from the

police?' "

-- Mr. Bulkeley is a staff reporter in The Wall Street Journal's Boston bureau.

Return to top of page

NEW FEATURES | SPECIAL REPORTS | GLOSSARY | PERSONAL FINANCE CENTER | TOOLS | CONTACT US | YOUR ACCOUNT | ADVERTISERS