



VI-2300 by Sanyo.<sup>®</sup>  
**FREE** \* with new 2-year agreement.  
\$189.99 without activation.  
\*After \$40 instant rebate. Offer valid through 1/21/06.

Buy Now ▶

[NYTimes.com](#)

Go to a Section ▾

SEARCH SPONSORED BY

SEARCH



All of Technology ▾

Search

[Technology Home](#)[Circuits](#)[Product Reviews](#)

## Waking Up to Recurring ID Nightmares

By TOM ZELLER Jr.

Published: January 9, 2006

AS members of Congress continue to dither over legislation concerning data security, the data broker industry, consumers' rights and identity theft - nearly a full year after the [ChoicePoint](#) debacle first woke Americans to the problem - perhaps they should meet Raymond Lorenzo.

[Skip to next paragraph](#)

*New York Times* technology reviewer David Pogue is at the 2006 Consumer Electronics Show, posting [blog entries](#) and daily [video updates](#).

In the early 1990's, someone ran amok, using Mr. Lorenzo's identity. It was used to rack up tens of thousands of dollars in fraudulent credit card debt. It was given to the police after various traffic violations. And a man even used the name Raymond Lorenzo when he was arrested and indicted in 1991 in Suffolk County, N.Y., for, among other things, burglary, forgery and criminal possession of a weapon.

That impostor, Peter Perro (the boyfriend of Mr. Lorenzo's ex-wife, it turned out), was additionally charged with criminal impersonation after Mr. Lorenzo filed a police report and fingerprints revealed the ruse. Mr. Perro was convicted on weapons and burglary charges in addition to criminal mischief.

But deep inside the state's Criminal Record Information Management System, it appears that a simple clerical error - and the digital ripples it unleashed - may have sealed a dismal future for Mr. Lorenzo.

"Lorenzo, Raymond" is listed as the felon, using the alias "Perro, Peter" - a perfect reversal of the facts.

The precise details are still being sorted out, but it seems clear that over the next 15 years, that digital nugget - like so much else in this age of consumer recordkeeping - was bought, sold, copied, stored, transmitted and appended to a digital dossier that, along with the erroneous debts and driving records, has haunted Mr. Lorenzo at every turn.

From New York to Florida, where he now lives, potential employers, landlords and even schools have pulled up those felonies on background checks of Mr. Lorenzo - one as recently as September - despite his many attempts to correct the record. Over the years, he has had to file for bankruptcy and has flirted with depression and debt stemming from \$30,000 in purchases he never made. His driver's license was revoked and he fought for two years to get it back - and five more to get points dropped from his record - all for violations he never committed.

At various turns, data brokers told him he could not see his dossier and that it could not be changed anyway. Bureaucratic court clerks told him there was little they could do.

"This whole thing has been worse than any nightmare I could ever have had for myself and my children," Mr. Lorenzo said in an e-mail message.

Last week, Mari J. Frank, an attorney in California and identity theft specialist who has been helping Mr. Lorenzo with his case, finally wrested a copy of the conviction record bearing the clerical goof from the Office of Court Administration in New York.

She hopes to file a motion to correct the record soon, although it could still take years for that information to make its way out of New York's criminal database and into every commercial silo that has ever compiled the erroneous information on Mr. Lorenzo.

"Identity theft is devastating for victims," Ms. Frank said. "Unfortunately, the companies and governmental agencies that facilitate this crime with sloppy information and handling practices have the money and clout to influence Congress to pass laws that protect themselves instead of our citizens."

That's assuming that Congress will ever manage to pass anything at all.

Since the giant data broker ChoicePoint announced last February that crooks had put information on 145,000 consumers at risk, the Privacy Rights Clearinghouse, an advocacy group in San Diego, has counted about 114 other major data breaches, affecting about 52 million Americans. This includes the disappearance just two weeks ago of backup tapes containing valuable data - including Social Security numbers and credit card information on more than 200,000 time-share owners - announced by [Marriott International](#).

"There needs to be better legislation," said George Waller, the executive vice president of StrikeForce Technologies, a company based in Edison, N.J. that develops identity verification technologies for governments, businesses and financial institutions.

"They say once the horse is out of the barn, why bother closing the door?" Mr. Waller said, referring to the millions of bits of consumer data already leaked into the black market. "But even if someone has your Social Security number, if you can prevent them from using it, that's the solution we should be driving towards."

Some states have been moving aggressively in that direction.

According to [Bankrate.com](http://Bankrate.com), which aggregates information on the financial industry, at least 10 states have enacted laws that allow consumers some ability to freeze their credit, which prevents a consumer reporting agency from releasing information without a consumer's direct authorization.

Had such a law existed in New York, it might have helped prevent Mr. Lorenzo's impostor from opening lines of credit in his name. A handful of proposals are currently pending in the State Assembly.

Indeed, the ChoicePoint scandal seemed to put the scare into the states. Last year, data breach legislation was introduced in at least 35 states and signed into law in at least 22, according to data compiled by the National Conference of State Legislatures.

Congress, on the other hand, introduced more than a dozen bills, but managed to reach consensus on none of them.

The problem is that data handlers want a narrow bill that would require them simply to notify consumers when a breach occurred and would give them broad discretion to decide when such a step was necessary. They would also prefer that any federal bill pre-empt the growing thicket of tough state laws.

Consumer and privacy rights advocates, on the other hand, want to preserve existing state laws while enacting broad federal notification standards, the ability to freeze credit, and new rights for consumers to see and correct information collected on them.

There is no question that Mr. Lorenzo - and perhaps millions of victims like him - might have been spared years of trouble had at least a few of those proposals been in place over the last decade of his life. Of course, whether those proposals will survive the cold calculus of realpolitik is an open question.

What is certain is that the debate on Capitol Hill will continue this year as surely as private information on thousands of consumers will continue to seep into the public sphere.

Just last week, [H&R Block](http://H&R Block) announced that it had mistakenly shipped some free copies of its tax software that compromised recipients' Social Security numbers: they were printed on the mailing labels.