

Chicago Tribune

BUSINESS

Flip over for
Careerbuilder

Data breaches persist despite security push

BY BECKY YERAK
Tribune reporter

Earlier this year, some employees of Schneider Electric of Palatine got an unwelcome surprise in a letter about the stock purchase plan in which they participate. Visible through the address window were their Social Security numbers.

One of Schneider's bulk mail vendors, it turned out, mistakenly exposed the sensitive data.

No Schneider employees have reported any instances of identity theft, the company says, but such data breaches remain a common tale.

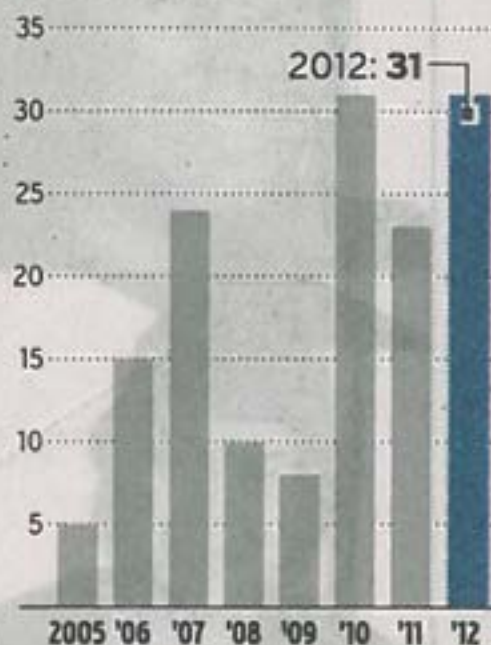
Despite rising awareness of cybersecurity, the number of incidents in which secure information is released into potentially untrustworthy environments remains nearly as high as ever by some measures worldwide and in Illinois.

In late April, LivingSocial, a rival of Chicago-based Groupon, disclosed that the names, email addresses and passwords of 50 million customers had been hacked.

Also last month, Roscoe resident Mary Akelaitis filed a class-action lawsuit

DATA BREACHES AT ILLINOIS INSTITUTIONS

Annual total



SOURCE: Privacy Rights Clearinghouse
TRIBUNE

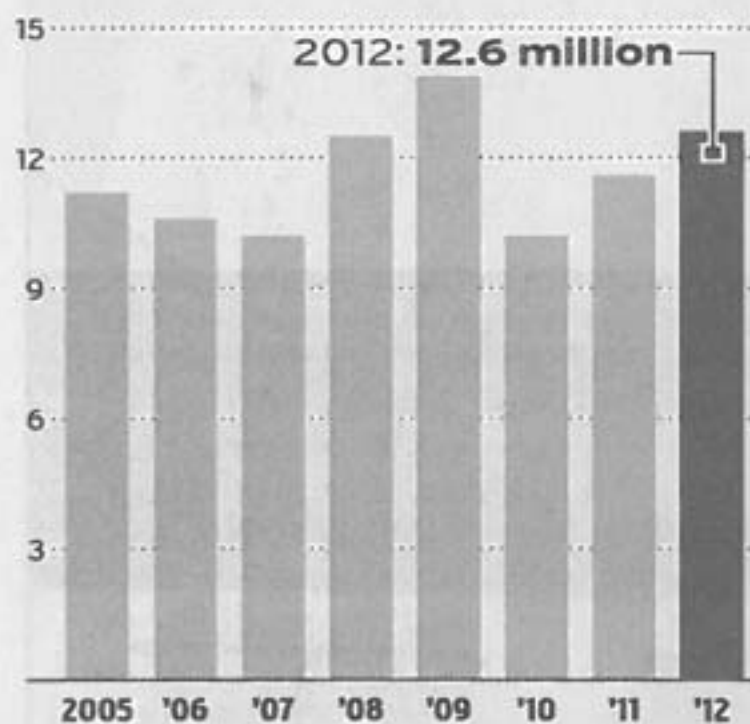
against Schnuck Markets Inc. The St. Louis-based retailer admitted that numbers and expiration dates of 2.4 million credit and debit cards used at most of its 100 stores — including those in Rockford — may have been exposed.

Rockford resident Tom Gwiazdowski fears that he and his wife were part of the Schnucks breach. They shop at the company's Hilander store on 11th Street in Rockford, and in late April they got a letter from their bank saying that their debit card had pos-

Please turn to Page 4

U.S. IDENTITY FRAUD VICTIMS

In millions



SOURCES: Javelin Strategy & Research
TRIBUNE

Continued from Page 1

sibly been compromised and that, for their security, it was being canceled.

"We're scared to death," said Gwiazdowski, who, like his wife, is blind. "We're so careful that we keep our cards in an aluminum wallet" because they believe it provides protection from identity thieves by blocking the chips imbedded in some credit cards. The couple has contacted St. Louis lawyer Jeff Millar, whose law firm has filed another class-action suit against Schnucks.

On April 15, the company said it's safe to shop at its stores.

Worldwide, 2,644 breaches were reported in 2012, more than double the 2011 number, according to the nonprofit Online Trust Alliance.

Last year, at least 31 Illinois institutions experienced data breaches, up by about 30 percent from the prior year and on par with 2010, according to a Tribune analysis of records compiled by the nonprofit Privacy Rights Clearinghouse, which typically compiles reported incidents affecting at least nine individuals.

Kristi Pearson, who works in billings for Chicago law firm Siprut PC, received an April 26 email from Living Social alerting her of the cyberattack.

"It's scary," she said. "The email tells you what they believe was compromised, but I don't know how much you can trust that."

Pearson's boss, Joseph Siprut, has litigated such privacy class actions as MedAssets' breach of Cook County Health system patient information, and PIN pad skimming cases involving Barnes & Noble and Michaels Stores.

Companies are being increasingly aggressive about collecting and monetizing consumers' personal information, he said, noting that the public doesn't always understand what they're giving up.

"When this information is aggregated, it poses substantial security risks, and yet the precautions that should accompany these data treasure troves have not really kept pace with the level of information collected," Siprut said. "That's why you can't go one week without reading a newspaper article about some new data breach."

Criminals are becoming more sophisticated, but chief data-breach causes include lost or stolen computing devices, employee errors and third-party mistakes, data protection researcher Ponemon Institute said recently. Improved productivity and convenience of mobile devices also make security more difficult.

Worse yet, a bigger percentage of data breaches are resulting in identity theft.

The number of identity fraud incidents nationwide in 2012 reached its highest level since 2009, and 1 in 4 data-breach letter recipients became identity fraud victims, Javelin Strategy & Research says. It used to be 20 percent.

At least eight incidents involving Illinois institutions have come to light in 2013. Here's a sample of some breaches: