08/01/2014

By John Breyault, Vice President of Public Policy, Telecommunications and Fraud – National Consumers League

Anyone who has watched the news over the past six months or so can attest that the issue of data security has now entered the mainstream conversation. Massive data breaches at nationally-known companies like Target, Michael's, Niemann Marcus and eBay – just to name a few – have brought the vulnerability of our nation's data security infrastructure home to millions of consumers.

It is NCL's strong belief that this issue has reached a turning point. At the same time that consumers are being asked to share ever-greater amounts of their personal data with companies, government and other entities, the capabilities of criminal hacking gangs has never been greater. Today, there are online black markets – some even offering 24/7 help desk support – where the budding cybercriminal can purchase consumers' credit or debit card information, their Social Security Number, email address and password and practically any other sensitive information a fraudster might want for a few dollars. This information is put to use on a daily basis defrauding consumers and businesses of billions – costs that are passed along to you and me through higher prices, inconvenience and difficulty in obtaining things like loans, tax refunds and even medical care.

Unfortunately, our nation's cyber defenses have not kept up with this threat. Globally last year more than 552 million identities were exposed by data breaches, according to Symantec, putting consumer's credit card information, birth dates, government ID numbers, home addresses, medical records, phone numbers, financial information, email addresses, login, passwords, and other personal information into the criminal underground.[1] Already in 2014, more than 360 breaches have been announced in the U.S. along, exposing more than 10.5 million customer records
[2]
, and that's just the breaches that have been made public.

It's with these sobering statistics in mind that NCL decided to launch the #DataInsecurity Project – to raise consumer and policymaker awareness of the urgent needs for reforms that

better protect consumer data from criminal hackers. Given the increasing scope and cost of data insecurity, consumers are speaking with one voice that Congress, our federal agencies, state and local governments and industry step up and take more responsibility for protecting consumers' sensitive information.

Consumers have had enough and they are calling for reform. A Javelin Strategy & Research poll found that 70 percent of fraud victims want the federal government to ensure that businesses meet basic data security standards. And 64 percent of victims believe that they should have the right to hold companies legally accountable when their information is compromised.

While there is no silver bullet to the problem of data insecurity, more can and should be done to secure consumers' sensitive information. The passage of a national data breach notification bill, modeled on California's strong law, would be a good start. Requiring mandatory data security standards for businesses that collect consumer data would be another pro-consumer step. Strengthening the authority of regulators like the Federal Trade Commission and increasing penalties for criminal hacking are also necessary in order to ensure a more secure data infrastructure.

Data insecurity is affecting consumer confidence in the marketplace, the ability of small businesses to compete, and trust in the Internet. The time for reform is now.

---

[1] http://www.symantec.com/connect/blogs/2013-internet-security-threat-report-year-mega-data-breach

[2] http://www.idtheftcenter.org/images/breach/ITRC_Breach_Stats_Report_2014.pdf