

**BUSINESSES MUST NOTIFY PUBLIC
OF COMPUTER SECURITY BREACH**

As of December 7, 2005, a new law will be in effect that requires businesses operating in New York state to publicly disclose any security breach of their computer systems that house personal information.

In the recent wake of high profile security breaches at ChoicePoint, Lexis/Nexis and CardSystems Solutions, New York is now among approximately 17 other states that have enacted similar laws designed to prevent the adverse consequences of identity theft.

Under the new law, businesses are required to notify individuals if certain personal information has been lost or stolen, such as Social Security numbers, driver's license numbers, or account or credit card numbers that are not encrypted. Disclosure could be triggered by an event as simple as an employee losing a computer that contains identifying information.

Notice must be given in writing but may be given electronically if the affected person "expressly" consented to electronic notice. If the cost of notification would exceed \$250,000, the business may provide the notice by (i) sending an e-mail to the affected person, if available, (ii) conspicuously posting notice on the

Business' Website, if it has one, and (iii) publishing the notice in a major statewide publication, such as a newspaper of statewide circulation.

The New York State Attorney General can bring an action for enforcement of the law on behalf of the state. A court may award damages for actual costs or losses, including consequential financial losses if a business violates the notification requirements recklessly or knowingly. This means that if a consumer loses money because of the security breach which could have been prevented if they were advised of the breach, the company who failed to provide the notice may have to pay those damages. A court may also award a civil penalty of the greater of \$5000 or up to \$10 per instance, with a maximum possible penalty of \$150,000.

The new law requires companies to seriously consider the adequacy of their computer security systems. As well, businesses should consider enacting policies and procedures to deal with the possibility that computerized personal information is stolen or lost. Of course the best way to deal with the new law is to avoid a breach in the first place, so an assessment to ensure that adequate security measures are in place is a must.

If you have any questions regarding the new law, please contact our attorneys below.

J. Montieth Estes*585.899.2949; mestes@jaeckle.com
 Joseph P. Kubarek*716.843.3862; jkubarek@jaeckle.com
 Jeffrey H. LaBarge*585.899.2954; jlabarge@jaeckle.com
 Mauri Aven Sankus*^o585.899.2953; maven@jaeckle.com
 Sharon P. Stiller*585.899.2934; sstillier@jaeckle.com
 James J. Tanous*716.843.3905; jtanous@jaeckle.com
 Susan J. Timian*585.899.2958; stimian@jaeckle.com

* Admitted to practice in New York State.

^o Admitted to practice in California and Pennsylvania.

JAECKLE FLEISCHMANN & MUGEL, LLP
www.jaeckle.com

BUFFALO

12 Fountain Plaza
Buffalo, NY 14202-2292
tel: 716.856.0600
fax: 716.856.0432

AMHERST

400 Essjay Road, Suite 320
Amherst, NY 14221-8228
tel: 716.250.1800
fax: 716.250.1806

ROCHESTER

190 Linden Oaks
Rochester, NY 14625-2812
tel: 585.899.2930
fax: 585.899.2931

PHOENIX

7047 E. Greenway Pkwy, Ste 250
Scottsdale, AZ 85254-8113
tel: 480.659.2213
fax: 480.659.3419