



June 13, 2007

Stephen. B. Nolan, Acting Director
Office of the Director
New Jersey Division of Consumer Affairs
124 Halsey Street
P.O. Box 45027
Newark, NJ 07101

**PROFESSIONAL
INSURANCE
AGENTS**

RE: Proposal Number: PRN 2007-116; Identity Theft Regulations

25 CHAMBERLAIN ST.
P. O. BOX 997
GLENMONT, NY 12077-0997
800/424-4244
FAX: 888/225-6935
WEB: www.pianj.org
E-MAIL: pia@pionline.org

PIANJ appreciates the opportunity to comment upon the division's proposed regulations to implement the Identity Theft Protection Act of 2005. PIANJ is a trade association that represents more than 7,000 professional independent insurance agents and their employees doing business in communities throughout New Jersey. These insurance agencies would be affected by the proposed regulations because insurance agencies obtain personal information to process insurance transactions for their customers.

PIANJ supports the goal of the regulations, which is to protect residents of New Jersey against identity theft. However, we believe that certain requirements go beyond the mandates of the authorizing statute and would impose an unreasonable burden upon small businesses, such as insurance agencies.

Computer system requirements

I. One size does not fill all

Section 13:45F-3.2 proposes an extensive list of computer system requirements that would apply to all businesses, no matter what the size. Many insurance agencies are small businesses with only a few employees and a few computers. Imposing these security system requirements on this type of business is simply not reasonable. Most insurance agencies would have to expend a considerable amount of time and money to implement the requirements, imposing an undue hardship on them.

The insurance industry is no stranger to the need to protect sensitive customer information. Insurance agencies are currently required by both state and federal privacy laws to implement an information security program that includes technical, administrative and physical safeguards to protect the security of confidential customer information.

These laws recognize that all businesses are not the same. Therefore, they require that the information security program "be appropriate to the size and complexity of the insurance entity and the nature and scope of the entity's activities."

PIANJ suggests that the division take a similar approach and recognize that smaller businesses should not be held to the same standard as larger ones.

II. Differing state requirements

PIANJ is also concerned that extensive state-specific requirements could be problematic for insurance agencies that do business in other states. Security breach laws have been enacted in several other states. If these states adopt regulations that impose their own computer system requirements, businesses could be faced with the problem of trying to comply with differing state requirements. Compliance would become a nightmare.

PIANJ suggests that the division not mandate the particular type of computer security systems that businesses use. Businesses should be allowed to develop their own security program, tailored to their own specific needs. The penalties imposed upon businesses that incur a security breach provide ample incentive for them to develop a security system that will protect their customer's personal information.

III. Specific concerns (13:45F-3.2)

Of particular concern to insurance agencies are the encryption requirements set forth in 13:45F-3.2(a)(3)(4) and (5). These requirements present an enormous challenge for the insurance industry in general, and in particular on smaller insurance agencies.

Currently, most insurance agencies utilize various agency management systems to process their daily insurance transactions. Most of these agency management systems do not employ encryption technology. Therefore, agencies would have to purchase encryption services from another vendor, which will be quite costly.

Further complications arise due to the requirement to employ encryption technology with respect to transmitted files. Insurance agencies communicate electronically with several different insurance companies with which they place business. It would be very difficult to encrypt information transmitted between insurance agencies and all the different insurance companies and other businesses with which they do business.

Subsection (a)(1) requires businesses to maintain security measures covering its computers, including any wireless system, which have secure user authentication access for all system components containing personal information including, control of user IDs and other identifiers and a secure method of assigning and selecting passwords consisting of at least seven letters and numbers.

PIANJ wishes to point out that it may be difficult for businesses to comply with respect to wireless systems, such as handheld devices (i.e. Blackberries). Various handheld wireless devices like IPAQ do not utilize authentication.

Also, the requirement for passwords to consist of at least seven letters and numbers would require many insurance companies to change their current passwords.

Subsection (a)(1)(ii) requires “control of user IDs...” Would the division clarify the meaning of this requirement?

Subsection (a)(1)(iii) restricts access to active users and active user accounts. This could be problematic for an insurance agency whose contract to write insurance for a particular company has been terminated. Although the insurance agency may not be writing new policies for a company, and thus not be an active user of the company’s system, the agency will have a continued need to access policyholder data contained on the insurance company’s computer system to service their customers and for other business reasons. If insurance companies must restrict access to active users, terminated insurance agents would be unable to obtain necessary policyholder information.

Subsection 10(iv) requires certain firewall configuration standards for businesses with more than five computers. The requirements under this subsection would be very expensive and should only apply to larger businesses, such as ones with more than 100 computers.

Subsection 11(iv) requires antispyware software that includes daily full system scans to ensure system integrity during off peak hours. This requirement seems unnecessary since antispyware performs active, real time scans. It would be redundant to run another scan at the end of the day. Additionally, if this scan is done during off hours, the computer would need to be left on after the close of business, which could pose a new security risk.

Subsection 19 requires encryption of all non-console administrative access. Would the division please clarify the meaning of this requirement.

Subsection 20 requires a process to render stored personal information unreadable wherever stored, including portable media and wireless networks. This requires a very high level of technology that most businesses do not currently employ, and it is not reasonable to require small businesses to employ this.

While PIANJ opposes the implementation of such overreaching security measures, if the division decides to adopt them, at the very least, it must give all businesses ample time to implement the changes. It could take years for insurance agencies, their system vendors and their insurance company partners to develop the technology that is required by this proposal.

Notification of security breach

Proposed section 13:45F-3.3(a) requires that businesses disclose to the State Police “any breach of security, regardless of the level of encryption or the presence of any security measures...”

This provision contradicts the definition of “breach of security” used in the proposal. There cannot be a “breach of security” as defined in the proposal, unless security measures or encryption are not used. Stated differently, can be no breach of security

where the data is encrypted. Thus, this section cannot require a report of a breach where data has been encrypted because a “breach of security” has not occurred under the proposal’s definition. Also, the statute defines “breach of security” as “unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.” Thus, the statute also provides that no breach of security has occurred if encryption has been used.

Also, the regulation calls for notice of the breach to be given to the State Police within six hours following discovery or notification of the breach. While PIANJ appreciates the need to act quickly in these matters, notification within six hours of discovery seems unreasonable. Businesses that discover a breach may need to gather facts and information to provide to the police. This would in many cases take longer than six hours.

Subsection (e)(2) requires that a notification of a breach include “a toll-free number that may be used to contact the business or public entity with any questions...” Many insurance agencies do not have toll-free telephone numbers. Instead of requiring a toll-free number, the division should consider requiring a cost-free method of contact, such as by e-mail.

Subsection (e)(4) requires a business to provide “information on how the affected individuals can protect themselves against, or limit the damage from identity theft or financial harm, including information about placing a fraud alert on the affected individual consumer report.” Insurance agencies should not be asked to become advisers to those whose identities may have been stolen. Nor, for that matter, should any business. PIANJ would not object if the proposal simply requires inclusion of information from another source, such as the FTC or IRS, on how individuals can protect themselves.

Mitigating damages

Proposed section 13:45F-3.1(d) would create a duty for businesses to mitigate the damages of a breach, even though the law does not impose such a requirement. Creating this new duty unreasonably exposes all businesses to even further liability in situations where damages for the breach itself could be quite costly.

Destruction of records

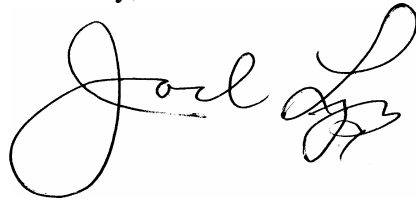
The statute requires that computer and paper records containing personal information that are no longer to be maintained be destroyed in such a manner that the information cannot be recreated. However, proposed 13:45F-3.5 goes far beyond that and requires that reports detailing what records were destroyed and how they were destroyed be maintained for 5 years. This seems to impose an unnecessary burden on businesses. Some businesses may want to protect themselves from litigation and may choose to document the methods of disposal of documents. However, this should not be a mandate.

Penalties

PIANJ believes that the penalties imposed by the regulation are excessive and unreasonable. Under 13:45F-5.2(b)(3) failure to maintain a computer security system as required by the regulation would be a violation of the Consumer Fraud Act, even if there has been no breach of security. This is simply too harsh a penalties for failing to meet such extensive computer system requirements.

Thank you for the opportunity to provide comments on this proposal. If you have any questions, you may contact me or PIANJ's Government Affairs Counsel, Jill Muratori.

Sincerely,

A handwritten signature in black ink, appearing to read "Jack Lynn". The signature is fluid and cursive, with a large initial "J" and a stylized "L".

Jack Lynn, CIC
PIANJ President