

**“BUSINESSES BEWARE—NEW FEDERAL LAW CAN MAKE YOU LIABLE
FOR YOUR CUSTOMER’S IDENTITY THEFT”**

© 2005 D. Daniel Engstrand, Jr.
By: D. Daniel Engstrand, Jr.
Doniger & Engstrand, LLP
12 Bayview Avenue
Northport, NY 11768
631.262.7400
dan@DandELAW.com

Effective June 1, 2005, all businesses, including restaurants, gas stations, retail stores, doctors, lawyers, in fact, anyone who obtains confidential personal information on its customers/clients, such as credit card information, in the normal course of its business, is now under a duty when disposing of it, to do so in such a fashion as to prevent it from getting into the hands of an identity thief. 16 C.F.R. §§682.3 and 682.5. Although this federal regulation does not require a business to dispose of such information, 16 C.F.R. §682.4, if a business does dispose of it, it must have procedures in place to safeguard this information. 16 C.F.R. §682.4.

Specifically, this new federal regulation requires that “[a]ny person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.” 16 C.F.R. §682.3(a). Under this rule, “[r]easonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following . . . (1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the

information cannot practicably be read or reconstructed. (2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.” 16 C.F.R. §682.3(b)(1) and (2).

Daly v. Metropolitan Life Ins. Co., 4 Misc.3d 887, 782 N.Y.S.2d 530 (Supreme Ct., New York County 2004), is illustrative of the monetary liabilities that can befall a business entity that fails to properly secure its clients’ confidential information. This case was decided a year prior to the federal regulation that became effective June 1, 2005. As part of its insurance application, Met Life required its customers to provide their full name, social security number, driver’s license number and date of birth. “Implicit in this agreement was a covenant to safeguard this information.” *Daly*, 4 Misc.3d at 893, 782 N.Y.S.2d at 535. Justice Walter Tolub ruled, in this case of first impression in New York, that the insurer, Metropolitan Life Insurance Company (hereinafter referred to as “Met Life”), had a duty to protect confidential personal information provided by its customers. *Id.* “[T]his court is convinced that Met Life had a duty to protect the confidential personal information provided by the plaintiffs.” *Id.* Therefore, even though a third party, the night janitor, stole the confidential information from Met Life’s computer data base, the court held that a sufficient claim of negligence was set forth to survive a summary judgment dismissal. *Id.*, 4 Misc.3d at 893-94, 782 N.Y.S.2d at 536. “Indeed, it is well established under New York law that ‘a fiduciary duty arises, even in a

commercial transaction, where one party reposed trust and confidence in another who exercises discretionary functions for the party’s benefit or possesses superior expertise on which the party relied. . . . ” *Id.*, 4 Misc.3d at 892, 782 N.Y.S.2d at 535 (citations omitted). Accordingly, the issue of monetary damages to be awarded and “whether Met Life’s responsibility for damages is lessened or eliminated under the theory that the theft of plaintiffs’ information by a third party was an unforeseeable intervening event are reserved as issues for trial.” *Id.*, 4 Misc.3d at 893-94, 782 N.Y.S.2d at 536.

The *Daly v. Met Life* case provides all business entities and professionals, who require as a conditional precedent to the establishment of a business/professional relationship that customers/clients provide them with confidential private information, fair warning that if they could be held liable for monetary damages should they fail to properly secure this information from access by a third party identity thief. Moreover, liability would conceivably be greater if the identity thief happened to be an employee of the business entity/professional.

Just because the identity thief may be judgment proof does not foreclose the consumer’s legal remedies to go after a “deep pocket” defendant who may have contributed to the identity theft. Under the new federal regulation and the *Daly v. Met Life* decision, that “deep pocket” would be the careless business owner who failed to implement proper disposal procedures to safeguard their customer’s confidential personal information from an identity thief.

A prudent business owner who maintains such confidential personal information should, in addition to the rule set forth in the new federal regulation, 16 C.F.R. §682.3, should also follow the analogous guidance set forth in the federal Health Insurance Portability and Accountability Act (“HIPAA”), as outlined by the United States Department of Health in 45 C.F.R. §164.530.¹ Doctors, hospitals and health insurance companies have had to follow these HIPAA guidelines to ensure the confidentiality of a patient’s medical records.

Essentially, a business should appoint a point person to be in charge of training its employees on the policies and procedures involved in protecting the confidentiality of a client’s/customer’s personal information. The training materials should be in writing. The confidential personal information collected on a client/customer should be safeguarded. Only those employees with a need to know a client’s/customer’s confidential personal information should be allowed access to it. Moreover, there must be a written policy in place outlining the business’ responsibility to investigate and respond to any violations of a client’s/customer’s confidential personal information. This policy must set forth the penalties for such violations and the employees’ obligation to report suspected violations to the point person. All employees must sign a written acknowledgement of having received the above training along with the written policies and procedures concerning the protection of a client’s confidential personal information and that they will fully abide by and maintain these policies and procedures. Furthermore, should any such violations occur, the business must document its investigation and findings as well as the penalties that it

administered and the fact that it immediately notified the police and other related authorities. In addition, the business must document the fact that it immediately notified the client/customer whose confidential personal information had been compromised, immediately upon learning of it. This will help to minimize any potential damage and loss to that client/customer and, ultimately, to the business, should it be named in a subsequent negligence lawsuit.

¹ **45 C.F.R. § 164.530 Administrative requirements.**

“(a)(1) Standard: Personnel designations.

(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) Implementation specification: Personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.

(2) Implementation specifications: Training.

(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2)(i) Implementation specification: Safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

(d)(1) Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures

required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.

(2) Implementation specification: Documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) Implementation specification: Documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) Standard: Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) Standard: Refraining from intimidating or retaliatory acts. A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

(1) Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;

(2) Individuals and others. Any individual or other person for:

(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;

(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

(h) Standard: Waiver of rights. A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) Standard: Policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) Standard: Changes to policies or procedures.

(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart;

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) Implementation specification: Changes in law. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must

promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) Implementation specifications: Changes to privacy practices stated in the notice.

(i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) Implementation specification: Changes to other policies or procedures. A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) Standard: Documentation. A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(2) Implementation specification: Retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

(k) Standard: Group health plans.

(1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

DONIGER & ENGSTRAND, LLP

“Businesses Beware—New Federal Law Can Make You Liable for Your Customer’s Identity Theft”, © 2005 D. Daniel Engstrand, Jr., Esq.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).”

Banks also have there own set of rules designed to protect and maintain the confidentiality of a customer’s personal information. See *e.g.*, 12 CFR 366.13 (bank employee’s obligation concerning confidential information), 12 CFR 978.6 (access to confidential privileged information)and 12 CFR 403.10 (Export/Import Bank regulations pertaining to national security information).