

Identity Theft—Fight Back and Erase the Damage

© 2006 D. Daniel Engstrand, Jr.

By D. Daniel Engstrand, Jr.

Doniger & Engstrand, LLP

12 Bayview Avenue

P.O. Box 575

Northport, NY 11768

631.262.7400

dan@DandELAW.com

www.DandELAW.com

In calendar year 2004, which is the latest year that identity theft statistics were reported by the Federal Trade Commission, there were 17,680 reported victims of identity theft in New York, ranking our state as the seventh (7th) highest in identity theft in states with 92 identity theft victims per 100,000 in population.¹ The news media is reporting, almost daily, large-scale identity thefts (i.e., *Newsday*, Being in the know on ID theft, April 15, 2005: compromised identity information from HSBC's North American division involving 180,000 customers, Bank of America affecting 1.2 million federal employees; breach of computer database at ChoicePoint affecting 145,000 people and stolen credit card numbers stolen from 103 DSW Warehouse stores). Last year, a Nassau County Detective was arrested and charged with using a fictitious name and social security number, provided to him for undercover narcotics work, to open credit accounts in which he made more than \$30,000.00 in fraudulent purchases.² In New York, the majority of identity theft crimes involve credit card fraud.³ Recognizing the insidious damage that identity theft is causing to our economy, President Bush declared the week of February 7, 2005, "National Consumer Protection Week".⁴

Up until as recently as December 7, 2005, businesses which regularly collected personal data on customers (i.e., credit card transactions, social security numbers, driver’s license information) were under no legal requirement to alert their customers when their computer databases which stored such confidential information had been compromised. With the enactment by the New York State Legislature of the Information Security Breach and Notification Act (hereinafter referred to as the “ISBNA”), effective December 7, 2005, such businesses must now immediately notify affected persons whenever there has been a breach of their confidential security computer system (for in-depth analysis, see pp.18-19, *infra*).

This article will focus on the various issues involved in restoring your good credit after having been victimized by identity theft. It will include reporting the theft to various government agencies, creditors/lenders and the credit reporting bureaus. Finally, this program will take you step by step on how to successfully litigate unresolved disputes in this area and what a business entity can do to protect itself from a claim that it negligently aided and abetted the identity theft by allowing its customers’ confidential personal information to become compromised.

The federal Fair Credit Billing Act limits responsibility for the unauthorized use of a credit card to fifty dollars (\$50.00), 15 U.S.C. §1643 (a)(1)(B).⁵ However, there are still certain procedures to follow to remove the adverse credit information from your credit history.⁶

Once you discover that you have been the victim of identity theft, you must immediately file a criminal complaint with your local police precinct. This is critical because you will need official documentary proof that you were a victim of identity theft for the particular credit transaction(s) set forth in the police report. As of 2002, New York has made identity theft a crime. See N.Y. Penal Law §§190.78 to 190.83.⁷ The New York Legislature has carefully carved out an exception to the identity theft crimes for persons under the age of twenty-one (21) years who use another’s identity solely to purchase alcohol, or, when under the age of eighteen (18) years, solely to purchase tobacco or to gain entrance to a place where there is an age restriction. N.Y. Penal Law §190.84.

Prior to the passage of these laws, some precincts would not issue a police report or would do so reluctantly.⁸ This made it difficult, if not impossible, to erase from your credit history the adverse credit information that resulted from the identity theft. The three main credit reporting bureaus (Equifax, Experian and Trans Union), as well as the creditors who issued credit to the identity thief, require proof that such a crime was committed before they will investigate a claim of identity theft. 15 U.S.C. §1681e makes the unauthorized disclosure of a credit report by a credit reporting agency itself a violation of the Fair Credit Reporting Act (see endnote 29, *infra*). A police report with its accompanying police case number should suffice as proof of the crime of identity theft. Many times, victims who were unable to file an identity theft report with the police would attempt to file a Miscellaneous Incident Report as documentary proof of the crime.

Now that identity theft has been made a crime in New York, the police must take your sworn complaint and issue a police report. Documentation is the key to proving that you were the victim of identity theft. Bring with you a current copy of your credit reports, collection letters and other documentation, if any, that would tend to prove that the particular transaction was not authorized.⁹ Contained within the police report is the accompanying police case number. Make certain to get a copy of the police report and case number. Also get the name, shield/badge and telephone number of the detective assigned to your case. “A law enforcement report containing detailed information about the identity theft and the signature, badge number or other identification information of the law enforcement official taking the report should be **sufficient on its face to support a victim’s request.**” 16 C.F.R. §603.3(c)(1)(emphasis added). Please take note that filing a false report of identity theft with the police is, in and of itself, a crime and may be prosecuted, accordingly. See N.Y. CPL §240.50 and 16 C.F.R. §603.3(a)(2).¹⁰

Armed with the police report and police case number, as documentary proof of the crime, you should next contact the identify theft department of each of the credit bureaus¹¹ as well as the credit issuer. Although the Fair Credit Reporting Act only requires you to notice one credit reporting agency and that agency, in turn, is required by law to notify all the other credit reporting agencies (see 15 U.S.C. §§1681c-1(a)(1)(B)), it is a good idea for you to contact each of them, immediately, along with the credit issuer involved in the fraudulent transaction. Contact all of them first by telephone and then follow up immediately

by letter sent certified mail along with a copy, not the original, of the police report and an original identity theft affidavit (see Attachment A).

The Fair Credit Billing Act protects the victim of credit card fraud by holding them liable only for the first fifty dollars (\$50.00), provided such fraud is reported to the card issuer in a timely fashion. 15 U.S.C. §1643 (a)(1)(B).¹² Bear in mind that the first fifty dollars (\$50.00) of liability is only limited to non-business credit card holders and to businesses where less than ten (10) employees have been issued a business credit card. If more than ten (10) employees have been issued a business credit card by the same credit issuer, then the business entity is responsible for the fraudulent transaction to the extent set forth in the contract between the issuer and the business. 15 U.S.C. §1645.¹³ However, in no event will the individual employee, whose card has been compromised, be liable for more than the first fifty dollars (\$50.00) of the fraudulent transaction. *Id.*

After you have reported the fraud to the credit card issuer to limit your liability to fifty dollars, you need to go about cleaning up the adverse credit information that more than likely now appears on your credit history. Therefore, you must contact the credit reporting bureaus (Equifax, Experian and Trans Union; see endnote 11, *infra*). Recently, the Fair Credit Reporting Act was amended to include 15 U.S.C. §1681c-1. This statutory subsection became effective on December 1, 2004. It requires a credit reporting agency to place a 90-day fraud alert on your file once you contact them to report “in good faith a suspicion “ that you have or are “about to become a victim of . . . identity theft”. 15 U.S.C. §1681c-1(a)(1).¹⁴ You can request that an extended fraud alert be

placed on your file for seven (7) years. To have an extended fraud alert placed on your file, you must provide the credit reporting agency with an “identity theft report”. 18 U.S.C. §1681c-1(b)(see endnote 14, *infra*). Essentially, an identity theft report means that you must provide the credit reporting bureau with a police report, *see supra*, and, in addition to that, a sworn affidavit that the particular transaction was not authorized by you. The FTC has prepared a sample “ID Theft Affidavit” to provide to companies and the credit reporting agencies (see Attachment A). A copy of the same may be obtained from the FTC website at www.consumer.gov/idtheft. Once there, click on “ID Theft Affidavit” on the left side of the screen and download the same.

By placing a fraud alert (extended fraud alert or active duty alert (for active duty military personnel which is good for two years) on your credit file with the credit reporting agency, it insures that

“[n]o prospective user of a consumer report . . . may establish a new credit plan or extension of credit, other than under an open-end credit plan^[15]. . . , in the name of the consumer, or issue an additional card on an existing credit account requested by a consumer, or grant any increase in credit limit on an existing credit account requested by a consumer, unless the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request.”

15 U.S.C. §1681c-1(h)(1)(B)(i).

Any adverse information resulting from the identity theft that appears in your credit file is automatically “blocked” and will not appear on the credit report within four (4) days of the credit reporting agency’s receipt of the following:

- “(1) appropriate proof of the identity of the consumer;
- (2) a copy of an identity theft report;
- (3) the identification of such information by the consumer; and

- (4) a statement by the consumer that the information is not information relating to any transaction by the consumer.”

15 U.S.C. §1681c-2.¹⁶

However, the credit reporting agency may decline or, if the block has already been effectuated, rescind the block if it determines that the “information was blocked in error” or that the consumer who requested the block made a “material misrepresentation of fact . . . relevant to the request to block” or received the “goods, services, or money as a result of the blocked transaction”.

15 U.S.C. §1681c-2(c)(1)(see endnote 16, *infra*). This can happen in a number of ways. It is unlikely that a credit reporting agency would decline or rescind a block, on its own, once it has been furnished with a copy of the police report and the identity theft affidavit. A credit reporting agency has a duty, when it prepares a credit report, to “follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.” 15 U.S.C. §1681(e)(b) (see endnote 29, *infra*). Willful violation of this statute would subject the credit reporting agency to actual and punitive damages and attorney’s fees. 15 U.S.C. §1681n (see endnote 25, *infra*). In addition, state penalties could be imposed on the credit reporting agency for violation of New York’s similar law, N.Y. General Business Law §380-j(e). “Consumer reporting agencies shall maintain reasonable procedures designed to assure maximum possible accuracy of the information concerning the individual about whom the report relates.” N.Y. Gen’l Bus. L. §3880-j(e). Therefore, what could happen, although unlikely, is that a credit provider, for whatever reason, may continue to dispute the claim of identity theft.

Remember, pursuant to 15 U.S.C. §1643, beyond the first fifty dollars, “a cardholder incurs no liability from the unauthorized use of a credit card.” 5 U.S.C. §1643(d). Moreover, “[i]n any action by a card issuer [Visa, Master Card, AMEX] to enforce liability for the use of a credit card, the burden of proof is upon the card issuer to show that the use was authorized.” *Id* at (b). Under the Fair Credit Billing Act, you have the right to contest the billing error (identity theft) directly with the creditor. 15 U.S.C. §1666.¹⁷ Once notified, the creditor has ninety (90) days in which to complete its investigation and either correct the account or send a written explanation which sets forth the reasons why the creditor believes the account statement was correct. 15 U.S.C. §1666(a)(B)(i) and (ii). If requested by the cardholder, the creditor must provide copies of the documentary evidence of the indebtedness. 15 U.S.C. §1666(a)(B)(ii). Be aware that if the claim is for goods not delivered or received, the burden is upon the creditor to prove that the goods were so received. *Id*. This is done by providing a statement of such determination that the goods were so received. *Id*.

During this ninety (90) day period in which the creditor is investigating the claim of a billing discrepancy and before its determination, no adverse credit information may be reported to any credit reporting agency by the creditor. 15 U.S.C. §1666a.¹⁸ Also, bear in mind that the card issuer (i.e., Visa, Master Card and AMEX) is subject to “all claims (other than tort claims) and defenses arising out of any transaction in which the credit card is used as a method of payment” 15 U.S.C. §1666i.¹⁹

More importantly, once a claim of identity theft has been made, “[n]o person shall sell, transfer for consideration, or place for collection a debt that such person has been notified under section 605B [15 U.S.C. §1681c-2] has resulted from identity theft.” 15 U.S.C. §1681m(f). This prohibition on debt collection applies to all debt collectors. *Id.*²⁰ In addition, once a claim of identity theft has been received by the creditor, the creditor may not report the adverse credit information pertaining to the theft to a credit reporting agency. 15 U.S.C. §1681s-2(a)(6).²¹ Furthermore, if the adverse information had previously been reported prior to receiving the claim of identity theft, the creditor must have procedures in place to prevent that blocked information from being resent to credit reporting agencies. *Id.*

The creditor is under an obligation, pursuant to the Fair Credit Reporting Act, to refrain from “furnish[ing] any information relating to a consumer to any consumer reporting agency if the [creditor] knows or has reasonable cause to believe that the information is inaccurate.” 15 U.S.C. §1681s-2(a)(1)(A). Moreover, that same section states, in pertinent part, that a creditor “shall not furnish information relating to a consumer to any consumer reporting agency if . . . the information is, in fact, inaccurate.” 15 U.S.C. §1681s-2(a)(1)(B). Unfortunately, there is no private cause of action for violation of this statute. 15 U.S.C. §1681s-2(c).

In addition, the Fair Credit Reporting Act imposes additional obligations upon the creditor that will aid the victim. Upon being placed on written notice of the claim of identity theft, the creditor must provide the victim with “a copy of [the]

application and business transaction records . . . evidencing any transaction alleged to be a result of identity theft. . . .” 15 U.S.C. §1681g(e)(1).²² This will usually provide the victim with proof that the credit transaction was unauthorized. It may also assist law enforcement in locating the whereabouts of the thief.

Should the creditor be unable to produce these records, such absence is “an affirmative defense (which the defendant [creditor] must establish by a preponderance of the evidence)” to be pleaded in any “civil action brought to enforce this subsection” that the creditor “has made a reasonably diligent search of its available business records” and “the records requested . . . do not exist or are not reasonably available.” 15 U.S.C. §1681g(e)(10)(see endnote 22, *infra*).

Think about this--the Fair Credit Reporting Act requires the creditor to produce these records. 15 U.S.C. §1681g(e)(1)(see endnote 22, *infra*). That same federal act requires the credit reporting agency to delete from its files any adverse credit information that cannot be verified. 15 U.S.C. §1681i(a)(5).²³ An argument can be made that the failure to produce (whether that failure be due to the destruction of records in the ordinary course of business or their unavailability) is tantamount to the failure to verify adverse credit information. Moreover, in a civil action to compel the creditor to produce such records, its failure could result in a spoliation of evidence charge.²⁴

Unfortunately, a victim cannot bring a civil cause of action for monetary damages against the creditor for its negligent and/or intentional failure to produce the thief’s fraudulent application and transaction records (15 U.S.C. §1681g(e)(6); see also, endnote 22, *infra*). The civil liability provisions of 15

U.S.C. §1681n²⁵ (intentional/willful violation of the Fair Credit Reporting Act) and 15 U.S.C. §1681o²⁶ (negligent violation of the Fair Credit Reporting Act) “do not apply to any violation of [15 U.S.C. §1681g(e)]”. 15 U.S.C. §1681g(e)(6) (see endnote 22, *infra*). However, a refusal by the credit reporting agency to delete the adverse credit information that cannot be verified because of the absence of such fraudulent application and transaction records could be deemed an intentional violation of the Fair Credit Reporting Act. See 15 U.S.C. §1681i(a)(5) (see endnote 23, *infra*) and 15 U.S.C. §1681g(c)(2)(E)²⁷. Such an intentional violation of the Fair Credit Reporting Act could subject the credit reporting agency, as well as the creditor, to civil liability under 15 U.S.C. §1681n (see endnotes 23 and 25, *infra*). Liability could consist of actual and punitive damages and attorney’s fees being imposed. 15 U.S.C. §1681n (see endnote 25, *infra*). Moreover, a credit reporting agency could be liable under state law. New York’s General Business Law §380-j(a)(3) prohibits a consumer reporting agency from reporting or maintaining in its files consumer information “which it has reason to know is inaccurate.”

So too can the reappearance of previously deleted adverse information subject the credit reporting agency to actual (not punitive) damages and attorney’s fees for negligence under 15 U.S.C. §1681o (see endnote 26, *infra*; see also, *Country Vanlines Inc. v. Experian Information Solutions, Inc.* 317 F. Supp.2d 383, 394 (S.D.N.Y. 2004). Just like the creditor, a credit reporting agency also has a corresponding duty to “maintain reasonable procedures designed to prevent the reappearance in a consumer’s file, and in consumer

reports on the consumer, of information that is deleted” 15 U.S.C. §1681i(a)(5)(C). However, a creditor cannot be subjected to civil liability in a private action for negligently allowing adverse information related to identity theft to reappear in a report to a credit reporting agency, 15 U.S.C. §1681s-2(c); a negligence cause of action lies only against the credit reporting agency.

Once the adverse information is deleted from the credit reporting agency’s file, it cannot be reinserted absent a certification from the creditor that the adverse information is accurate and the consumer has been notified. 15 U.S.C. §1681i(a)(5)(B)(i) and (ii) (see endnote 23, *infra*). Moreover, the credit reporting agency must “maintain reasonable procedures designed to prevent the reappearance in a consumer’s file, and in consumer reports on the consumer, of information that is deleted” 15 U.S.C. §1681i(a)(5)(C) (see endnote 23, *infra*).

After undoubtedly having spent numerous hours and having incurred significant legal fees in correcting the damage done to your credit, you may want to consider whether it is worthwhile to bring a lawsuit for money damages for all the aggravation that this theft of your identity has caused you. Chances are the perpetrator of this crime has no assets, making a civil lawsuit against him/her impracticable. Just because the thief may be judgment proof does not foreclose your legal remedies to go after “deep pocket” defendants who may have contributed to the identity theft.

How did the thief obtain your private/privileged information?²⁸ *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 failed to properly secure its clients' confidential information. *Daly* predates the enactment of ISBNA (see pp.18-19, *infra*). 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. *Daly*, 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. . . ." *Daly*, 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.” *Daly*, 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 condition 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 under the common law 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.

Likewise, a credit reporting agency, pursuant to the Fair Credit Reporting Act, may not furnish a person’s credit report to a creditor unless authorized. 15 U.S.C. §1681e.²⁹ The wrongful disclosure of a credit report could subject the credit reporting agency to an action seeking actual and punitive damages, pursuant to 15 U.S.C. §1681n (“willful noncompliance with the Fair Credit Reporting Act; see endnote 25, *infra*). Such a wrongful disclosure claim was raised in *TRW, Inc. v. Adelaid Andrews*, 534 U.S. 19, 122 S.Ct. 441, 151 L.Ed.2d 339 (2001).

In that case, Adelaid Andrews visited a radiologist. The doctor’s office required that before performing any services that Adelaid Andrews complete a form listing her name, social security number, birth date and other private information. As it turns out, the receptionist at that office, Andrea Andrews, copied this information and moved to Las Vegas. Once in Vegas, Andrea

Andrews attempted to open credit accounts using Adelaid Andrew’s social security number in her own name. It was only when Adelaid Andrews, two years later, attempted to refinance her home that she learned of the identity theft. Needless to say, the damage to her credit was done and Adelaid Andrews was unable to refinance her home with the low rate that she would have had her credit not been tarnished by the identity theft.

TRW was named as a defendant in that litigation because every time a “company from which the Impostor sought credit requested a report from TRW . . . , TRW’s computers registered a match between Andrews’ Social Security number, last name, and first initial and therefore responded by furnishing her file.” TRW, Inc., 534 U.S. at 24, 122 S.Ct. at 445, 151 L.Ed.2d at 345. Plaintiff sought punitive damages from TRW, pursuant to 15 U.S.C. §1681n (“willful noncompliance with the Fair Credit Reporting Act; see endnote 25, *infra*) for wrongfully disclosing her credit report in response to the identity thief’s request for credit. Adelaid Andrews sued TRW more than two years after the unauthorized disclosure of her credit report by TRW.

Fortunately for TRW, at the time of that action, the statute of limitations for violations under the Fair Credit Reporting Act were limited to two (2) years; there was no “general discovery rule” that would have expanded the two-year limitation period by allowing it to run from the date of discovery, rather than from the time of the occurrence. Since that decision, Congress had amended the statute of limitations to include a “general discovery rule”. Accordingly, today, the statute of limitations for violations of the Fair Credit Reporting Act begins to run from two

(2) years from the date of discovery and, in no event, more than five (5) years from the date of the occurrence.³⁰ Why Adelaid Andrews did not sue the radiologist's office for its negligence in failing to properly secure her confidential personal information is not known. Perhaps she did bring such an action in state court and it was subsequently settled without being reported.

Today, a federal regulation, effective June 1, 2005, has codified the duty imposed upon a business by the common law to protect personal/confidential information from unauthorized access. 16 C.F.R. §682.3(a) requires, in pertinent part, 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). See *also*, 16 C.F.R. §682.5. Under that 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).

This regulation affects any one or any entity doing business that maintains customer/client confidential personal information. Thus, a prudent business owner who maintains such confidential personal information should, in addition to the rule set forth in 16 C.F.R. §682.3, also follow the analogous guidance set forth in the federal Health Insurance Portability and Accountability Act, as outlined by the United States Department of Health in 45 C.F.R. §164.530.³¹

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.

New York has recently enacted the Information Security Breach and Notification Act (hereinafter referred to as the “ISBNA”). 2005 N.Y. Laws 442. The ISBNA amended New York’s Technology Law and General Business Law to provide an immediate notification requirement whenever any state governmental or private business computer database containing personal/confidential information (i.e., social security numbers, credit card information, driver’s license information) has been compromised by an unauthorized user. Until the enactment of the ISBNA, companies whose databases have been compromised by hackers were not required to report this breach of security. To date, there is no federal counterpart to the ISBNA.

Effective December 7, 2005, N.Y. Technology Law §208³² now requires any New York State entity and N.Y. General Business Law §899-aa³³ now requires any private person or business which conducts business in New York to immediately disclose any breach by an unauthorized user of their computer database which contains confidential personal information to all affected New York residents. Although local municipal entities are exempted from N.Y. Technology Law §208, that statute nevertheless still requires local governments to adopt their own local notification policy or law “consistent with [N.Y.

Technology Law §208]” no later than April 6, 2006. N.Y. Technology Law §208(8).

As of this writing, neither Suffolk nor Nassau Counties have adopted such a local law or policy. Suffolk’s Local Law Chapter 656, enacted on May 17, 2005 (prior to the enactment of the ISBNA), comes the closest, but still does not adhere to the notification requirement of N.Y. Technology Law §208. Suffolk County Local Law Chapter 656 states, in pertinent part, the following:

“It shall be the policy of the Suffolk County government to institute any and all procedures that would achieve the following goals:

- A. Maintain the confidentiality of personal information, including but not limited to names, addresses, telephone numbers, and social security numbers, to the maximum extent possible under the law.
- B. Refrain from acquiring or maintaining lists of names, addresses, telephone numbers, and social security numbers of County residents, unless absolutely required for some legal or governmental purpose.”

Suffolk County Local Law Chapter 656.

There is no penalty provision for violation of N.Y. Technology Law §208 by a state or local government. However, that is not the case for a violation of the notification requirements by a private business under N.Y. Gen’l Bus. Law §899-aa. Failure by a private business person or entity to make this required notification will subject the violator to an injunction as well as “actual costs or losses incurred by a person entitled to notice . . . , if notification was not provided . . . , including consequential financial losses” in an action brought by the New York State Attorney General. N.Y. Gen’l Bus. Law §899-aa(6)(a). Civil penalties ranging from \$5,000.00 to \$150,000.00 could also be imposed against the private business violator, if it was found to have intentionally or recklessly violated this

disclosure law. *Id.* It is unclear whether a private right of action will be allowed under General Business Law §899-aa.

It must be remembered that in most cases involving an allegation of identity theft, a credit reporting company will delete and correct any adverse information relating to the identity theft from your file. However, in those rare cases where this has not been done, to prevail on any action against the credit reporting company, you must prove a willful and/or negligent violation of the Fair Credit Reporting Act under 15 U.S.C. §§1681n and 1681o (see endnotes 25 and 26, *infra*). Both the federal and state courts have jurisdiction over Fair Credit Reporting Act claims without regard to the amount in controversy. 15 U.S.C. §1681p (see endnote 30, *infra*). Moreover, state defamation, privacy and negligent reporting claims are preempted by the Fair Credit Reporting Act's shield of qualified immunity. 15 U.S.C. §1681h(e).³⁴ Malice or willful intent is required to defeat qualified immunity. *Id.* Therefore, to maintain a defamation action against a credit reporting agency, either a showing of common law malice (spite or ill-will) or Constitutional malice (defamatory statement made with a high degree of awareness of its probable falsity—a reckless disregard for the truth) must be made to pierce the qualified immunity enjoyed by the credit agency. See *Country Vanlines Inc. v. Experian Information Solutions, Inc.*, 317 F.Supp.2d 383 (S.D.N.Y. 2004).

Finally, if you know the perpetrator of this crime, you may go after him or her for your actual and punitive damages. Chances are, though, that this individual does not have a proverbial pot to go after. If the thief is part of a large

conspiracy with assets to go after, you may consider bringing a civil RICO action, although the likelihood of you recovering from some organized crime syndicate is more than likely nonexistent for the private litigant.

RICO, which stands for the Racketeer Influence and Corrupt Organizations, allows you to recover treble damages, costs and attorneys fees. Racketeering activity has been defined by the criminal RICO statute to include identity theft. 18 U.S.C. §1961(1)(B).³⁵ It is unlawful, under the criminal RICO statutes, “for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise’s affairs through a pattern of racketeering activity. . . .” 18 U.S.C. §1962(c)³⁶. A “pattern of racketeering activity” has been defined under RICO to require “at least two acts of racketeering activity” within ten (10) years of each other. 18 U.S.C. §1961(5). That same statute defines an “enterprise” as being “any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity. . . .” 18 U.S.C. §1961(4).

The civil RICO statute provides, in pertinent part, that “[a]ny person injured in his business or property by reason of a violation of [the criminal RICO statutes, 18 U.S.C. §§1961, *et seq.*] may sue therefore in any appropriate United States district court and shall recover threefold the damages he sustains and the cost of the suit, including a reasonable attorney’s fee” 18 U.S.C. §1964(c). Therefore, if you can tie the thief to any “enterprise”, as that term is defined by

RICO (18 U.S.C. §1961(4)), then you may consider bringing a civil RICO action against that person. More than likely, it will be the criminal RICO statutes that will be used in the prosecution of the criminal action.

Nevertheless, there are a number of ways that you can protect yourself against identity theft. A recently enacted federal statute which goes into effect on December 4, 2006, will protect the consumer by requiring credit card machines and cash registers to truncate all credit card receipts. 15 U.S.C. §1681c(g). Until then, be careful. Many companies still give receipts with the full credit card number listed. Therefore, shred all credit card receipts to prevent identity theft through dumpster diving.

California has a state law that allows anyone, not just a victim of identity theft, to place a freeze on their entire credit history. This is the ultimate preventative measure for preventing identity theft. A freeze will prevent a creditor to review an applicant's credit history. This should prevent new credit accounts from being opened, until the freeze is lifted. Texas has a similar law which only allows identity theft victims to place a freeze on their credit history. New York does not have such a law nor is one being contemplated by either house in the state legislature.

Finally, ascertain whether your card issuer can provide you with a virtual account number for internet purchases. What this means is that when entering your credit card number on-line, instead of your actual number appearing, a substitute number will appear in place of your real credit card number. However, all purchases will appear in your monthly statement as having been made

against your actual card number. This will protect your actual account number from being stolen on-line.

Another useful tip to protect yourself is to monitor your credit reports regularly. Effective September 1, 2005, all residents in New York are eligible to obtain annually, free of charge, a copy of their credit reports from Equifax, Experian and Trans Union. To do this, go on-line to www.annualcreditreport.com. Since you are only entitled to one free report per year from each of these credit reporting agencies, you may want to consider staggering your requests over the year.

In conclusion, the best way to protect yourself is to prevent identity theft from happening altogether.

¹ Federal Trade Commission (hereinafter referred to as the “FTC”) Identity Theft Victim Complaint Data, Figures and Trends in New York, January 1-December 31, 2004 at Figure 4a, *Identity Theft Victims by State*, obtained from the FTC website www.consumer.gov. Arizona, Nevada, California, Texas, Colorado and Florida were ranked by the FTC as number 1 through 6, respectively. In terms of actual numbers of victims, New York (17,680 victims) would rank as the third highest state in identity theft behind California (43,839 victims) and Texas (26,454 victims). *Id.*

² *Newsday*, June 2, 2005, cover story, LI Cop’s Alias: Thief.

³ FTC Identity Theft Victim Complaint Data, Figures and Trends in New York, January 1-December 31, 2004 at Figure 1, obtained from the FTC website www.consumer.gov.

⁴ 3 CFR Proclamation 7979
Proclamation 7979 of February 8, 2006--National Consumer Protection Week, 2006

“A Proclamation by the President of the United States of America

During National Consumer Protection Week, we highlight the importance of consumer education in the ongoing fight against fraud and encourage consumers to make wise decisions.

Each year, nearly 25 million adults are victims of consumer fraud. These crimes damage lives and shake consumer confidence. The Federal Trade Commission (FTC) and other organizations recommend several steps that Americans can take to help protect themselves against fraud. First, consumers should be cautious about giving out personal information such as Social Security and account numbers. Second, they should be aware of the credentials of an organization before making a transaction, especially through the

mail, over the phone, or on the Internet. Third, before finalizing a purchase or agreement, the FTC suggests considering offers with care, avoiding immediate decisions, and requesting to have information in writing. In addition, when using the Internet, the FTC recommends that consumers exercise caution in responding to solicitations and that consumers use and regularly update their anti-virus software and firewall.

My Administration is committed to vigorous enforcement of the consumer protection statutes, and the Department of Justice's Office of Consumer Litigation and other Federal agencies are working diligently to that end. The FTC is working to fight unsolicited e-mail under the Controlling the Assault of Non-Solicited Pornography and Marketing Act and is establishing new rules under the Fair and Accurate Credit Transactions Act to further protect against identity theft. We are protecting American consumers through the National Do-Not-Call Registry.

Millions of Americans have registered already, and individuals may call 1-888-382-1222 or visit the Do-Not-Call website at www.donotcall.gov to have their number added to the list. Citizens can learn more about ways to fight fraud from the National Consumer Protection Week website at www.consumer.gov/ncpw. By actively guarding against fraud, consumers can protect themselves and enhance the strength and integrity of our Nation's economy.

NOW, THEREFORE, I, GEORGE W. BUSH, President of the United States of America, by virtue of the authority vested in me by the Constitution and laws of the United States, do hereby proclaim February 5 through February 11, 2006, as National Consumer Protection Week. I call upon Government officials, industry leaders, and consumer advocates to provide citizens with information about how they can be responsible consumers, and I encourage all citizens to take an active role in protecting their personal information.

IN WITNESS WHEREOF, I have hereunto set my hand this third day of February, in the year of our Lord two thousand six, and of the Independence of the United States of America the two hundred and thirtieth.

GEORGE W. BUSH”

⁵ Some credit issuers will not even hold you responsible for the first fifty dollars (i.e., American Express Fraud Protection Guarantee and Visa's Zero Liability policy, both of which guarantee not to hold you responsible for any fraudulent transaction, including the first fifty dollars).

⁶ You have an obligation to examine your monthly credit card statements. Failure to do so which allowed the fraud to go undetected beyond the month in which it first appeared is negligence and could result in the cardholder being liable for fraudulent charges that he/she allowed to continue beyond that first month. *Minskoff v. American Exp. Travel Related Svcs.*, 98 F.3d 703, 709 (2d Cir. 1996). “the negligent acts or omissions of a cardholder may create apparent authority to use the card in a person who obtained the card through theft or fraud.” *Id.* The United States Court of Appeals sitting in New York analogized the cardholder's obligation to examine and timely report any fraud that may appear in his/her statement with that of a consumer who is required, under the N.Y. Unif. Comm. Code §4-406(1), to examine bank statements.

⁷ **N.Y. Penal Law §190.78 Identity theft in the third degree**

”A person is guilty of identity theft in the third degree when he or she knowingly and with

intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, and thereby:

1. obtains goods, money, property or services or uses credit in the name of such other person or causes financial loss to such person or to another person or persons; or
 2. commits a class A misdemeanor or higher level crime.
- Identity theft in the third degree is a class A misdemeanor.”

N.Y. Penal Law §190.79 Identity theft in the second degree

”A person is guilty of identify theft in the second degree when he or she knowingly and with intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, and thereby:

1. obtains goods, money, property or services or uses credit in the name of such other person in an aggregate amount that exceeds five hundred dollars; or
 2. causes financial loss to such person or to another person or persons in an aggregate amount that exceeds five hundred dollars; or
 3. commits or attempts to commit a felony or acts as an accessory to the commission of a felony; or
 4. commits the crime of identity theft in the third degree as defined in section 190.78 of this article and has been previously convicted within the last five years of identity theft in the third degree as defined in section 190.78, identity theft in the second degree as defined in this section, identity theft in the first degree as defined in section 190.80, unlawful possession of personal identification information in the third degree as defined in section 190.81, unlawful possession of personal identification information in the second degree as defined in section 190.82, unlawful possession of personal identification information in the first degree as defined in section 190.83, grand larceny in the fourth degree as defined in section 155.30, grand larceny in the third degree as defined in section 155.35, grand larceny in the second degree as defined in section 155.40 or grand larceny in the first degree as defined in section 155.42 of this chapter.
- Identity theft in the second degree is a class E felony.”

N.Y. Penal Law §190.80 Identity theft in the first degree

”A person is guilty of identity theft in the first degree when he or she knowingly and with intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, and thereby:

1. obtains goods, money, property or services or uses credit in the name of such other person in an aggregate amount that exceeds two thousand dollars; or
2. causes financial loss to such person or to another person or persons in an aggregate amount that exceeds two thousand dollars; or
3. commits or attempts to commit a class D felony or higher level crime or acts as an accessory in the commission of a class D or higher level felony; or
4. commits the crime of identity theft in the second degree as defined in section 190.79 of this article and has been previously convicted within the last five years of identity theft in the third degree as defined in section 190.78, identity theft in the second degree as defined in section 190.79, identity theft in the first degree as defined in this section, unlawful possession of personal identification information in the third degree as defined in section 190.81, unlawful possession of personal identification information in the second degree as defined in section 190.82, unlawful possession of personal identification information in the first degree as defined in section 190.83, grand larceny in the fourth degree as defined in section 155.30, grand larceny in the third degree as defined in

section 155.35, grand larceny in the second degree as defined in section 155.40 or grand larceny in the first degree as defined in section 155.42 of this chapter.
Identity theft in the first degree is a class D felony.”

N.Y. Penal Law §190.81 Unlawful possession of personal identification information in the third degree

”A person is guilty of unlawful possession of personal identification information in the third degree when he or she knowingly possesses a person’s financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother’s maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person knowing such information is intended to be used in furtherance of the commission of a crime defined in this chapter.

Unlawful possession of personal identification information in the third degree is a class A misdemeanor.”

N.Y. Penal Law §190.82 Unlawful possession of personal identification information in the second degree

”A person is guilty of unlawful possession of personal identification information in the second degree when he or she knowingly possesses two hundred fifty or more items of personal identification information of the following nature: a person’s financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother’s maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person knowing such information is intended to be used in furtherance of the commission of a crime defined in this chapter.

Unlawful possession of personal identification information in the second degree is a class E felony.”

N.Y. Penal Law §190.83 Unlawful possession of personal identification information in the first degree

”A person is guilty of unlawful possession of personal identification information in the first degree when he or she commits the crime of unlawful possession of personal identification information in the second degree and:

1. with intent to further the commission of identity theft in the second degree, he or she supervises more than three accomplices; or
2. he or she has been previously convicted within the last five years of identity theft in the third degree as defined in section 190.78, identity theft in the second degree as defined in section 190.79, identity theft in the first degree as defined in section 190.80, unlawful possession of personal identification information in the third degree as defined in section 190.81, unlawful possession of personal identification information in the second degree as defined in section 190.82, unlawful possession of personal identification information in the first degree as defined in this section, grand larceny in the fourth degree as defined in section 155.30, grand larceny in the third degree as defined in section 155.35, grand larceny in the second degree as defined in section 155.40 or grand larceny in the first degree as defined in section 155.42 of this chapter.

Unlawful possession of personal identification information in the first degree is a class D felony.”

⁸ As of 1970, Congress had enacted the precursor to an identity theft statute, 15 U.S.C. §1644. That statute made the fraudulent use of a credit card in the amount of \$1,000.00 a crime with a 10-year prison term and/or a fine of \$10,000.00. However, that statute did not address the misappropriation of another’s identity. It was not until 1998 when Congress passed the Identity Theft and Assumption Deterrence Act, 18 U.S.C. §1028, that the theft of one’s identity became a federal crime. In pertinent part, 18 U.S.C. §1028 states, that it is a federal crime when one “knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit . . . any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. . . .” 18 U.S.C. §1028(a)(7). There is no private right of action under 18 U.S.C. §10228. *Garay v. U.S. Bancorp.*, 303 F.Supp.2d 299, 302 (E.D.N.Y. 2004). In 2004, Congress passed the Identity Theft Penalty Enhancement Act, 18 U.S.C. §1028A. This statute provides additional sentences, ranging from 2 to 5 years to be imposed, consecutively. See *also* 18 U.S.C. §1029 (fraud in connection with access devices or device-making equipment).

⁹ Excellent websites to search for preventive and corrective tips in the area of identity theft are the FTC’s websites (www.ftc.gov/idtheft) and (www.consumer.gov/idtheft); Identity Theft Resource Center website (www.idtheftcenter.org); Privacy Rights Clearinghouse website (www.privacyrights.org); Victims Assistance of America website (www.victimsassistanceofamerica.org); and the Nassau County Police Department’s website (www.police.co.nassau.ny.us).

¹⁰ **N.Y. Penal Law § 240.50 Falsely reporting an incident in the third degree**

“A person is guilty of falsely reporting an incident in the third degree when, knowing the information reported, conveyed or circulated to be false or baseless, he:

1. Initiates or circulates a false report or warning of an alleged occurrence or impending occurrence of a crime, catastrophe or emergency under circumstances in which it is not unlikely that public alarm or inconvenience will result; or
2. Reports, by word or action, to an official or quasi-official agency or organization having the function of dealing with emergencies involving danger to life or property, an alleged occurrence or impending occurrence of a catastrophe or emergency which did not in fact occur or does not in fact exist; or
3. Gratuitously reports to a law enforcement officer or agency (a) the alleged occurrence of an offense or incident which did not in fact occur; or (b) an allegedly impending occurrence of an offense or incident which in fact is not about to occur; or (c) false information relating to an actual offense or incident or to the alleged implication of some person therein; . . .

Falsely reporting an incident in the third degree is a class A misdemeanor.”

16 C.F.R. §603.3(a)(2) states, in pertinent part, that

“[t]he term ‘identity theft report’ means a report . . . [t]hat is a copy of an official, valid report filed by the consumer with a Federal, State, or local law enforcement agency, including the United States Postal Inspection Service, **the filing of which subjects the person filing the report to criminal penalties relating to the filing of false information, if, in fact, the information in the report is false . . .**”

16 C.F.R. §603.3(a)(2)(emphasis added).

¹¹ Equifax can be contacted on line at www.equifax.com and their Fraud Alert Department may be reached at P.O. Box 740201, Atlanta, GA 30374-0241 or by telephone at 1.800.525.6285; Experian can be contacted on line at www.experian.com and their Fraud Alert Department may be reached at P.O. Box 9532, Allen, TX 75013 or by telephone at 1.888.397.3742; Trans Union

can be contacted on line at www.transunion.com and their Fraud Alert Department may be reached at P.O. Box 6790, Fullerton, CA 92634-6790 or by telephone at 1.800.680.7289.

¹² **15 U.S.C. § 1643. Liability of holder of credit card**

”(a) Limits on liability.

(1) A cardholder shall be liable for the unauthorized use of a credit card only if—

(A) the card is an accepted credit card;

(B) the liability is not in excess of \$ 50;

(C) the card issuer gives adequate notice to the cardholder of the potential liability;

(D) the card issuer has provided the cardholder with a description of a means by which the card issuer may be notified of loss or theft of the card, which description may be provided on the face or reverse side of the statement required by section 127(b) [15 USCS 1637(b)] or on a separate notice accompanying such statement;

(E) the unauthorized use occurs before the card issuer has been notified that an unauthorized use of the credit card has occurred or may occur as the result of loss, theft, or otherwise; and

(F) the card issuer has provided a method whereby the user of such card can be identified as the person authorized to use it.

(2) For purposes of this section, a card issuer has been notified when such steps as may be reasonably required in the ordinary course of business to provide the card issuer with the pertinent information have been taken, whether or not any particular officer, employee, or agent of the card issuer does in fact receive such information.

(b) Burden of proof. In any action by a card issuer to enforce liability for the use of a credit card, the burden of proof is upon the card issuer to show that the use was authorized or, if the use was unauthorized, then the burden of proof is upon the card issuer to show that the conditions of liability for the unauthorized use of a credit card, as set forth in subsection (a), have been met.

(c) Liability imposed by other laws or by agreement with issuer. Nothing in this section imposes liability upon a cardholder for the unauthorized use of a credit card in excess of his liability for such use under other applicable law or under any agreement with the card issuer.

(d) Exclusiveness of liability. Except as provided in this section, a cardholder incurs no liability from the unauthorized use of a credit card.”

15 U.S.C. §1643 (emphasis added).

¹³ **15 U.S.C. § 1645. Business credit cards; limits on liability of employees**

“. . . a card issuer and a business or other organization which provides credit cards issued by the same card issuer to ten or more of its employees may by contract agree as to liability of the business or other organization with respect to unauthorized use of such credit cards without regard to the provisions of section 133 [15 USCS § 1643], but in no case may such business or other organization or card issuer impose liability upon any employee with respect to unauthorized use of such a credit card except in accordance with and subject to the limitations of section 133 [15 USCS § 1643].”

¹⁴ **15 U.S.C. § 1681c-1. Identity theft prevention; fraud alerts and active duty alerts**

(a) One-call fraud alerts.

(1) Initial alerts. Upon the direct request of a consumer, or an individual acting on behalf of or as a personal representative of a consumer, who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, a consumer reporting agency described in section 1681a(p) of this title that maintains a file on the consumer and has received appropriate proof of the identity of the requester shall--

(A) include a fraud alert in the file of that consumer, and also provide that alert along with any credit score generated in using that file, for a period of not less than 90 days, beginning on the date of such request, unless the consumer or such representative requests that such fraud alert be removed before the end of such period, and the agency has received appropriate proof of the identity of the requester for such purpose; and

(B) refer the information regarding the fraud alert under this paragraph to each of the other consumer reporting agencies described in section 1681a(p) of this title, in accordance with procedures developed under section 1681s(f) of this title.

(2) Access to free reports. In any case in which a consumer reporting agency includes a fraud alert in the file of a consumer pursuant to this subsection, the consumer reporting agency shall--

(A) disclose to the consumer that the consumer may request a free copy of the file of the consumer pursuant to section 1681j(d) of this title; and

(B) provide to the consumer all disclosures required to be made under section 1681a of this title, without charge to the consumer, not later than 3 business days after any request described in subparagraph (A).

(b) Extended alerts.

(1) In general. Upon the direct request of a consumer, or an individual acting on behalf of or as a personal representative of a consumer, who submits an identity theft report to a consumer reporting agency described in section 1681a(p) of this title that maintains a file on the consumer, if the agency has received appropriate proof of the identity of the requester, the agency shall--

(A) include a fraud alert in the file of that consumer, and also provide that alert along with any credit score generated in using that file, during the 7-year period beginning on the date of such request, unless the consumer or such representative requests that such fraud alert be removed before the end of such period and the agency has received appropriate proof of the identity of the requester for such purpose;

(B) during the 5-year period beginning on the date of such request, exclude the consumer from any list of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance to the consumer as part of a transaction that was not initiated by the consumer, unless the consumer or such representative requests that such exclusion be rescinded before the end of such period; and

(C) refer the information regarding the extended fraud alert under this paragraph to each of the other consumer reporting agencies described in section 1681a(p) of this title, in accordance with procedures developed under section 1681s(f) of this title.

(2) Access to free reports. In any case in which a consumer reporting agency includes a fraud alert in the file of a consumer pursuant to this subsection, the consumer reporting agency shall--

(A) disclose to the consumer that the consumer may request 2 free copies of the file of the consumer pursuant to section 1681j(d) of this title during the 12-month period beginning on the date on which the fraud alert was included in the file; and

(B) provide to the consumer all disclosures required to be made under section 1681g of this title, without charge to the consumer, not later than 3 business days after any request described in subparagraph (A).

(c) Active duty alerts. Upon the direct request of an active duty military consumer, or an individual acting on behalf of or as a personal representative of an active duty military consumer, a consumer reporting agency described in section 1681a(p) of this title that maintains a file on the active duty military consumer and has received appropriate proof of the identity of the requester shall--

(1) include an active duty alert in the file of that active duty military consumer, and also provide that alert along with any credit score generated in using that file, during a period of not less than 12 months, or such longer period as the Commission shall determine, by regulation, beginning on the date of the request, unless the active duty military consumer or such representative requests that such fraud alert be removed before the end of such period, and the agency has received appropriate proof of the identity of the requester for such purpose;

(2) during the 2-year period beginning on the date of such request, exclude the active duty military consumer from any list of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance to the consumer as part of a transaction that was not initiated by the consumer, unless the consumer requests that such exclusion be rescinded before the end of such period; and

(3) refer the information regarding the active duty alert to each of the other consumer reporting agencies described in section 1681a(p) of this title, in accordance with procedures developed under section 1681s(f) of this title.

(d) Procedures. Each consumer reporting agency described in section 1681a(p) of this title shall establish policies and procedures to comply with this section, including procedures that inform consumers of the availability of initial, extended, and active duty alerts and procedures that allow consumers and active duty military consumers to request initial, extended, or active duty alerts (as applicable) in a simple and easy manner, including by telephone.

(e) Referrals of alerts. Each consumer reporting agency described in section 1681a(p) of this title that receives a referral of a fraud alert or active duty alert from another consumer reporting agency pursuant to this section shall, as though the agency received the request from the

consumer directly, follow the procedures required under--

(1) paragraphs (1)(A) and (2) of subsection (a), in the case of a referral under subsection (a)(1)(B) of this section;

(2) paragraphs (1)(A), (1)(B), and (2) of subsection (b) of this section, in the case of a referral under subsection (b)(1)(C) of this section; and

(3) paragraphs (1) and (2) of subsection (c) of this section, in the case of a referral under subsection (c)(3) of this section.

(f) Duty of reseller to reconvey alert. A reseller shall include in its report any fraud alert or active duty alert placed in the file of a consumer pursuant to this section by another consumer reporting agency.

(g) Duty of other consumer reporting agencies to provide contact information. If a consumer contacts any consumer reporting agency that is not described in section 1681a(p) of this title to communicate a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, the agency shall provide information to the consumer on how to contact the Commission and the consumer reporting agencies described in section 1681a(p) of this title to obtain more detailed information and request alerts under this section.

(h) Limitations on use of information for credit extensions.

(1) Requirements for initial and active duty alerts.

(A) Notification. Each initial fraud alert and active duty alert under this section shall include information that notifies all prospective users of a consumer report on the consumer to which the alert relates that the consumer does not authorize the establishment of any new credit plan or extension of credit, other than under an open-end credit plan (as defined in section 1602(i) of this title), in the name of the consumer, or issuance of an additional card on an existing credit account requested by a consumer, or any increase in credit limit on an existing credit account requested by a consumer, except in accordance with subparagraph (B).

(B) Limitation on users.

(i) In general. No prospective user of a consumer report that includes an initial fraud alert or an active duty alert in accordance with this section may establish a new credit plan or extension of credit, other than under an open-end credit plan (as defined in section 1602(i) of this title), in the name of the consumer, or issue an additional card on an existing credit account requested by a consumer, or grant any increase in credit limit on an existing credit account requested by a consumer, unless the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request.

(ii) Verification. If a consumer requesting the alert has specified a telephone number to be used for identity verification purposes, before authorizing any new credit plan or extension described in clause (i) in the name of such consumer, a user of such consumer report shall contact the consumer using that telephone number or take reasonable steps to verify the consumer's identity and confirm that the application for a new credit plan is not the result of identity theft.

(2) Requirements for extended alerts.

(A) Notification. Each extended alert under this section shall include information that provides all prospective users of a consumer report relating to a consumer with--

(i) notification that the consumer does not authorize the establishment of any new credit plan or extension of credit described in clause (i), other than under an open-end credit plan (as defined in section 1602(i) of this title), in the name of the consumer, or issuance of an additional card on an existing credit account requested by a consumer, or any increase in credit limit on an existing credit account requested by a consumer, except in accordance with subparagraph (B); and

(ii) a telephone number or other reasonable contact method designated by the consumer.

(B) Limitation on users. No prospective user of a consumer report or of a credit score generated using the information in the file of a consumer that includes an extended fraud alert in accordance with this section may establish a new credit plan or extension of credit, other than under an open-end credit plan (as defined in section 1602(i) of this title), in the name of the consumer, or issue an additional card on an existing credit account requested by a consumer, or any increase in credit limit on an existing credit account requested by a consumer, unless the user contacts the consumer in person or using the contact method described in subparagraph (A)(ii) to confirm that the application for a new credit plan or increase in credit limit, or request for an additional card is not the result of identity theft.”

(emphasis added).

¹⁵ “The term ‘open end credit plan’ means a plan under which the creditor reasonably contemplates repeated transactions, which prescribes the terms of such transactions, and which provides for a finance charge which may be computed from time to time on the outstanding unpaid balance. A credit plan which is an open end credit plan within the meaning of the preceding sentence is an open end credit plan even if credit information is verified from time to time.”

15 U.S.C. §1602(i). Meaning, if you already have a typical VISA, Master Charge or AMEX credit card, you may continue to use it and the credit issuer may continue to extend credit to you on the existing account on a monthly as needed basis, despite the fraud alert.

¹⁶ **15 USCS § 1681c-2. Block of information resulting from identity theft**

“(a) Block

Except as otherwise provided in this section, a consumer reporting agency shall block the reporting of any information in the file of a consumer that the consumer identifies as information that resulted from an alleged identity theft, not later than 4 business days after the date of receipt by such agency of—

(1) appropriate proof of the identity of the consumer;

(2) a copy of an identity theft report;

(3) the identification of such information by the consumer; and

(4) a statement by the consumer that the information is not information relating to any transaction by the consumer.

(b) Notification

A consumer reporting agency shall promptly notify the furnisher of information identified by the consumer under subsection (a)—

- (1) that the information may be a result of identity theft;
- (2) that an identity theft report has been filed;
- (3) that a block has been requested under this section; and
- (4) of the effective dates of the block.

(c) Authority to decline or rescind

- (1) In general

A consumer reporting agency may decline to block, or may rescind any block, of information relating to a consumer under this section, if the consumer reporting agency reasonably determines that—

(A) the information was blocked in error or a block was requested by the consumer in error;

(B) the information was blocked, or a block was requested by the consumer, on the basis of a material misrepresentation of fact by the consumer relevant to the request to block; or

(C) the consumer obtained possession of goods, services, or money as a result of the blocked transaction or transactions.

- (2) Notification to consumer

If a block of information is declined or rescinded under this subsection, the affected consumer shall be notified promptly, in the same manner as consumers are notified of the reinsertion of information under section 1681i(a)(5)(B) of this title.

- (3) Significance of block

For purposes of this subsection, if a consumer reporting agency rescinds a block, the presence of information in the file of a consumer prior to the blocking of such information is not evidence of whether the consumer knew or should have known that the consumer obtained possession of any goods, services, or money as a result of the block.

(d) Exception for resellers

- (1) No reseller file

This section shall not apply to a consumer reporting agency, if the consumer reporting agency—

(A) is a reseller;

(B) is not, at the time of the request of the consumer under subsection (a), otherwise furnishing or reselling a consumer report concerning the information identified by the consumer; and

(C) informs the consumer, by any means, that the consumer may report the identity theft to the Commission to obtain consumer information regarding identity theft.

- (2) Reseller with file

The sole obligation of the consumer reporting agency under this section, with regard to any request of a consumer under this section, shall be to block the consumer report maintained by the consumer reporting agency from any subsequent use, if—

(A) the consumer, in accordance with the provisions of subsection (a), identifies, to a consumer reporting agency, information in the file of the consumer that resulted from identity theft; and

(B) the consumer reporting agency is a reseller of the identified information.

- (3) Notice

In carrying out its obligation under paragraph (2), the reseller shall promptly provide a notice to the consumer of the decision to block the file. Such notice shall contain the name, address, and telephone number of each consumer reporting agency from which the consumer information was obtained for resale.

(e) Exception for verification companies

The provisions of this section do not apply to a check services company, acting as such, which issues authorizations for the purpose of approving or processing negotiable instruments, electronic fund transfers, or similar methods of payments, except that, beginning 4 business days after receipt of information described in paragraphs (1) through (3) of subsection (a), a check services company shall not report to a national consumer reporting agency described in section 1681a(p) of this title, any information identified in the subject identity theft report as resulting from identity theft.

(f) Access to blocked information by law enforcement agencies

No provision of this section shall be construed as requiring a consumer reporting agency to prevent a Federal, State, or local law enforcement agency from accessing blocked information in a consumer file to which the agency could otherwise obtain access under this title [15 USCS §§ 1681 et seq.]”

15 U.S.C.S. §1681c-2

¹⁷ **15 U.S.C. § 1666. Correction of billing errors**

“(a) Written notice by obligor to creditor; time for and contents of notice; procedure upon receipt of notice by creditor

If a creditor, within sixty days after having transmitted to an obligor a statement of the obligor's account in connection with an extension of consumer credit, receives at the address disclosed under section 1637(b)(10) of this title a written notice (other than notice on a payment stub or other payment medium supplied by the creditor if the creditor so stipulates with the disclosure required under section 1637(a)(7) of this title) from the obligor in which the obligor—

(1) sets forth or otherwise enables the creditor to identify the name and account number (if any) of the obligor,

(2) indicates the obligor's belief that the statement contains a billing error and the amount of such billing error, and

(3) sets forth the reasons for the obligor's belief (to the extent applicable) that the statement contains a billing error,

the creditor shall, unless the obligor has, after giving such written notice and before the expiration of the time limits herein specified, agreed that the statement was correct—

(A) not later than thirty days after the receipt of the notice, send a written acknowledgment thereof to the obligor, unless the action required in subparagraph (B) is taken within such thirty-day period, and

(B) not later than two complete billing cycles of the creditor (in no event later than ninety days) after the receipt of the notice and prior to taking any action to collect the amount, or any part thereof, indicated by the obligor under paragraph (2) either—

(i) make appropriate corrections in the account of the obligor, including the crediting of any finance charges on amounts erroneously billed, and transmit to the obligor a notification of such corrections and the creditor's explanation of any change in the amount indicated by the obligor under

paragraph (2) and, if any such change is made and the obligor so requests, copies of documentary evidence of the obligor's indebtedness; or

(ii) send a written explanation or clarification to the obligor, after having conducted an investigation, setting forth to the extent applicable the reasons why the creditor believes the account of the obligor was correctly shown in the statement and, upon request of the obligor, provide copies of documentary evidence of the obligor's indebtedness. In the case of a billing error where the obligor alleges that the creditor's billing statement reflects goods not delivered to the obligor or his designee in accordance with the agreement made at the time of the transaction, a creditor may not construe such amount to be correctly shown unless he determines that such goods were actually delivered, mailed, or otherwise sent to the obligor and provides the obligor with a statement of such determination.

After complying with the provisions of this subsection with respect to an alleged billing error, a creditor has no further responsibility under this section if the obligor continues to make substantially the same allegation with respect to such error.

(b) Billing error

For the purpose of this section, a "billing error" consists of any of the following:

(1) A reflection on a statement of an extension of credit which was not made to the obligor or, if made, was not in the amount reflected on such statement.

(2) A reflection on a statement of an extension of credit for which the obligor requests additional clarification including documentary evidence thereof.

(3) A reflection on a statement of goods or services not accepted by the obligor or his designee or not delivered to the obligor or his designee in accordance with the agreement made at the time of a transaction.

(4) The creditor's failure to reflect properly on a statement a payment made by the obligor or a credit issued to the obligor.

(5) A computation error or similar error of an accounting nature of the creditor on a statement.

(6) Failure to transmit the statement required under section 1637(b) of this title to the last address of the obligor which has been disclosed to the creditor, unless that address was furnished less than twenty days before the end of the billing cycle for which the statement is required.

(7) Any other error described in regulations of the Board.

(c) Action by creditor to collect amount or any part thereof regarded by obligor to be a billing error

For the purposes of this section, "action to collect the amount, or any part thereof, indicated by an obligor under paragraph (2)" does not include the sending of statements of account, which may include finance charges on amounts in dispute, to the obligor following written notice from the obligor as specified under subsection (a), if—

(1) the obligor's account is not restricted or closed because of the failure of the obligor to pay the amount indicated under paragraph (2) of subsection (a), and

(2) the creditor indicates the payment of such amount is not required pending the creditor's compliance with this section.

Nothing in this section shall be construed to prohibit any action by a creditor to collect any amount which has not been indicated by the obligor to contain a billing error.

(d) Restricting or closing by creditor of account regarded by obligor as containing a billing error

Pursuant to regulations of the Board, a creditor operating an open end consumer credit plan may not, prior to the sending of the written explanation or clarification required under paragraph (B)(ii), restrict or close an account with respect to which the obligor has indicated pursuant to subsection (a) that he believes such account to contain a billing error solely because of the obligor's failure to pay the amount indicated to be in error. Nothing in this subsection shall be deemed to prohibit a creditor from applying against the credit limit on the obligor's account the amount indicated to be in error.

(e) Effect of noncompliance with requirements by creditor

Any creditor who fails to comply with the requirements of this section or section 1666a of this title forfeits any right to collect from the obligor the amount indicated by the obligor under paragraph (2) of subsection (a) of this section, and any finance charges thereon, except that the amount required to be forfeited under this subsection may not exceed \$ 50."

15 U.S.C. §1666.

¹⁸ **15 U.S.C. §1666a. Regulation of credit reports**

"(a) Reports by creditor on obligor's failure to pay amount regarded as billing error

After receiving a notice from an obligor as provided in section 1666(a) of this title, a creditor or his agent may not directly or indirectly threaten to report to any person adversely on the obligor's credit rating or credit standing because of the obligor's failure to pay the amount indicated by the obligor under section 1666(a)(2) of this title, and such amount may not be reported as delinquent to any third party until the creditor has met the requirements of section 1666 of this title and has allowed the obligor the same number of days (not less than ten) thereafter to make payment as is provided under the credit agreement with the obligor for the payment of undisputed amounts.

(b) Reports by creditor on delinquent amounts in dispute; notification of obligor of parties notified of delinquency

If a creditor receives a further written notice from an obligor that an amount is still in dispute within the time allowed for payment under subsection (a) of this section, a creditor may not report to any third party that the amount of the obligor is delinquent because the obligor has failed to pay an amount which he has indicated under section 1666(a)(2) of this title, unless the creditor also reports that the amount is in dispute and, at the same time, notifies the obligor of the name and address of each party to whom the creditor is reporting information concerning the delinquency.

(c) Reports by creditor of subsequent resolution of delinquent amounts

A creditor shall report any subsequent resolution of any delinquencies reported pursuant to subsection (b) to the parties to whom such delinquencies were initially reported."

15 U.S.C. §1666a.

¹⁹ **15 U.S.C. § 1666i. Assertion by cardholder against card issuer of claims and defenses arising out of credit card transaction;**

prerequisites; limitation on amount of claims or defenses

“(a) Claims and defenses assertible

Subject to the limitation contained in subsection (b), a card issuer who has issued a credit card to a cardholder pursuant to an open end consumer credit plan shall be subject to all claims (other than tort claims) and defenses arising out of any transaction in which the credit card is used as a method of payment or extension of credit if (1) the obligor has made a good faith attempt to obtain satisfactory resolution of a disagreement or problem relative to the transaction from the person honoring the credit card; (2) the amount of the initial transaction exceeds \$50; and (3) the place where the initial transaction occurred was in the same State as the mailing address previously provided by the cardholder or was within 100 miles from such address, except that the limitations set forth in clauses (2) and (3) with respect to an obligor's right to assert claims and defenses against a card issuer shall not be applicable to any transaction in which the person honoring the credit card (A) is the same person as the card issuer, (B) is controlled by the card issuer, (C) is under direct or indirect common control with the card issuer, (D) is a franchised dealer in the card issuer's products or services, or (E) has obtained the order for such transaction through a mail solicitation made by or participated in by the card issuer in which the cardholder is solicited to enter into such transaction by using the credit card issued by the card issuer.

(b) Amount of claims and defenses assertible

The amount of claims for defenses asserted by the cardholder may not exceed the amount of credit outstanding with respect to such transaction at the time the cardholder first notifies the card issuer or the person honoring the credit card of such claim or defense. For the purpose of determining the amount of credit outstanding in the preceding sentence, payments and credits to the cardholder's account are deemed to have been applied, in the order indicated, to the payment of: (1) late charges in the order of their entry to the account; (2) finance charges in order of their entry to the account; and (3) debits to the account other than those set forth above, in the order in which each debit entry to the account was made.”

15 U.S.C. §1666i.

²⁰ There is no private right of redress for violation of 15 U.S.C. §1681m. 15 U.S.C. §1681m(h)(8). Therefore, if a creditor attempted to have a debt collector recover a debt claimed to be the result of identity theft, a clear violation of 15 U.S.C. §1681m(f), no civil action could be brought by the aggrieved party. 15 U.S.C. §1681m(h)(8)

²¹ 15 U.S.C. §1681s-2(a)(6) states, in pertinent part, the following:

“Duties of furnishers upon notice of identity theft-related information

(A) Reasonable procedures. A person that furnishes information to any consumer reporting agency shall have in place reasonable procedures to respond to any notification that it receives from a consumer reporting agency under section 1681c-2 of this title relating to information resulting from identity theft, to prevent that person from refurnishing such blocked information.

(B) Information alleged to result from identity theft

If a consumer submits an identity theft report to a person who furnishes information to a consumer reporting agency at the address specified by that person for receiving such reports stating that information maintained by such

person that purports to relate to the consumer resulted from identity theft, the person may not furnish such information that purports to relate to the consumer to any consumer reporting agency, unless the person subsequently knows or is informed by the consumer that the information is correct.”

15 U.S.C. §1681s-2(a)(6).

²² **15 U.S.C. §1681g(e) Information available to victims.**

“(1) In general

For the purpose of documenting fraudulent transactions resulting from identity theft, not later than 30 days after the date of receipt of a request from a victim in accordance with paragraph (3), and subject to verification of the identity of the victim and the claim of identity theft in accordance with paragraph (2), a business entity that has provided credit to, provided for consideration products, goods, or services to, accepted payment from, or otherwise entered into a commercial transaction for consideration with, a person who has allegedly made unauthorized use of the means of identification of the victim, shall provide a copy of application and business transaction records in the control of the business entity, whether maintained by the business entity or by another person on behalf of the business entity, evidencing any transaction alleged to be a result of identity theft to—

(A) the victim;

(B) any Federal, State, or local government law enforcement agency or officer specified by the victim in such a request; or

(C) any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of records provided under this subsection.

(2) Verification of identity and claim

Before a business entity provides any information under paragraph (1), unless the business entity, at its discretion, otherwise has a high degree of confidence that it knows the identity of the victim making a request under paragraph (1), the victim shall provide to the business entity—

(A) as proof of positive identification of the victim, at the election of the business entity--

(i) the presentation of a government-issued identification card;

(ii) personally identifying information of the same type as was provided to the business entity by the unauthorized person; or

(iii) personally identifying information that the business entity typically requests from new applicants or for new transactions, at the time of the victim's request for information, including any documentation described in clauses (i) and (ii); and

(B) as proof of a claim of identity theft, at the election of the business entity—

(i) a copy of a police report evidencing the claim of the victim of identity theft; and

(ii) a properly completed—

(I) copy of a standardized affidavit of identity theft developed and made available by the Commission; or

(II) an affidavit of fact that is acceptable to the business entity for that purpose.

(3) Procedures

The request of a victim under paragraph (1) shall—

(A) be in writing;

(B) be mailed to an address specified by the business entity, if any;
and

(C) if asked by the business entity, include relevant information about any transaction alleged to be a result of identity theft to facilitate compliance with this section including—

- (i) if known by the victim (or if readily obtainable by the victim), the date of the application or transaction; and
- (ii) if known by the victim (or if readily obtainable by the victim), any other identifying information such as an account or transaction number.

(4) No charge to victim

Information required to be provided under paragraph (1) shall be so provided without charge.

(5) Authority to decline to provide information

A business entity may decline to provide information under paragraph (1) if, in the exercise of good faith, the business entity determines that—

- (A) this subsection does not require disclosure of the information;
- (B) after reviewing the information provided pursuant to paragraph (2), the business entity does not have a high degree of confidence in knowing the true identity of the individual requesting the information;
- (C) the request for the information is based on a misrepresentation of fact by the individual requesting the information relevant to the request for information; or
- (D) the information requested is Internet navigational data or similar information about a person's visit to a website or online service.

(6) Limitation on liability

Except as provided in section 1681s of this title, sections 1681n and 1681o of this title do not apply to any violation of this subsection.

(7) Limitation on civil liability

No business entity may be held civilly liable under any provision of Federal, State, or other law for disclosure, made in good faith pursuant to this subsection.

(8) No new recordkeeping obligation

Nothing in this subsection creates an obligation on the part of a business entity to obtain, retain, or maintain information or records that are not otherwise required to be obtained, retained, or maintained in the ordinary course of its business or under other applicable law.

(9) Rule of construction

(A) In general

No provision of, prohibiting the disclosure of financial information by a business entity to third parties shall be used to deny disclosure of information to the victim under this subsection.

(B) Limitation

Except as provided in subparagraph (A), nothing in this subsection permits a business entity to disclose information, including information to law enforcement under subparagraphs (B) and (C) of paragraph (1), that the business entity is otherwise prohibited from disclosing under any other applicable provision of Federal or State law.

(10) Affirmative defense

In any civil action brought to enforce this subsection, it is an affirmative defense (which the defendant must establish by a preponderance of the evidence) for a business entity to file an affidavit or answer stating that—

- (A) the business entity has made a reasonably diligent search of its available business records; and
- (B) the records requested under this subsection do not exist or are not reasonably available.

(11) Definition of victim. For purposes of this subsection, the term "victim" means a consumer whose means of identification or financial information has been used or transferred (or has been alleged to have been used or transferred) without the authority of that consumer, with the intent to commit, or to aid or abet, an identity theft or a similar crime.

(12) Effective date

This subsection shall become effective 180 days after December 4, 2003.

(13) Effectiveness study.

Not later than 18 months after December 4, 2003, the Comptroller General of the United States shall submit a report to Congress assessing the effectiveness of this provision."

15 U.S.C. §1681g(e).

²³ **15 U.S.C. §1681i. Procedure in case of disputed accuracy**

"(a) Reinvestigations of disputed information

(1) Reinvestigation required.—

(A) In general.—Subject to subsection (f), if the completeness or accuracy of any item of information contained in a consumer's file at a consumer reporting agency is disputed by the consumer and the consumer notifies the agency directly, or indirectly through a reseller, of such dispute, the agency shall, free of charge, conduct a reasonable reinvestigation to determine whether the disputed information is inaccurate and record the current status of the disputed information, or delete the item from the file in accordance with paragraph (5), before the end of the 30-day period beginning on the date on which the agency receives the notice of the dispute from the consumer or reseller.

(B) Extension of period to reinvestigate.—Except as provided in subparagraph (C), the 30-day period described in subparagraph (A) may be extended for not more than 15 additional days if the consumer reporting agency receives information from the consumer during that 30-day period that is relevant to the reinvestigation.

(C) Limitations on extension of period to reinvestigate.—

Subparagraph (B) shall not apply to any reinvestigation in which, during the 30-day period described in subparagraph (A), the information that is the subject of the reinvestigation is found to be inaccurate or incomplete or the consumer reporting agency determines that the information cannot be verified.

(2) Prompt notice of dispute to furnisher of information.—

(A) In general.—Before the expiration of the 5-business-day period beginning on the date on which a consumer reporting

agency receives notice of a dispute from any consumer or a reseller in accordance with paragraph (1), the agency shall provide notification of the dispute to any person who provided any item of information in dispute, at the address and in the manner established with the person. The notice shall include all relevant information regarding the dispute that the agency has received from the consumer or reseller.

(B) Provision of other information.—The consumer reporting agency shall promptly provide to the person who provided the information in dispute all relevant information regarding the dispute that is received by the agency from the consumer or the reseller after the period referred to in subparagraph (A) and before the end of the period referred to in paragraph (1)(A).

(3) Determination that dispute is frivolous or irrelevant.—

(A) In general.—Notwithstanding paragraph (1), a consumer reporting agency may terminate a reinvestigation of information disputed by a consumer under that paragraph if the agency reasonably determines that the dispute by the consumer is frivolous or irrelevant, including by reason of a failure by a consumer to provide sufficient information to investigate the disputed information.

(B) Notice of determination.—Upon making any determination in accordance with subparagraph (A) that a dispute is frivolous or irrelevant, a consumer reporting agency shall notify the consumer of such determination not later than 5 business days after making such determination, by mail or, if authorized by the consumer for that purpose, by any other means available to the agency.

(C) Contents of notice.—A notice under subparagraph (B) shall include—

(i) the reasons for the determination under subparagraph (A); and

(ii) identification of any information required to investigate the disputed information, which may consist of a standardized form describing the general nature of such information.

(4) Consideration of consumer information.—In conducting any reinvestigation under paragraph (1) with respect to disputed information in the file of any consumer, the consumer reporting agency shall review and consider all relevant information submitted by the consumer in the period described in paragraph (1)(A) with respect to such disputed information.

(5) Treatment of inaccurate or unverifiable information.—

(A) In general. If, after any reinvestigation under paragraph (1) of any information disputed by a consumer, an item of the information is found to be inaccurate or incomplete or cannot be verified, the consumer reporting agency shall--

(i) promptly delete that item of information from the file of the consumer, or modify that item of information, as appropriate, based on the results of the reinvestigation; and

(ii) promptly notify the furnisher of that information that the information has been

modified or deleted from the file of the consumer.

(B) Requirements relating to reinsertion of previously deleted material.—

(i) Certification of accuracy of information.—If any information is deleted from a consumer's file pursuant to subparagraph (A), the information may not be reinserted in the file by the consumer reporting agency unless the person who furnishes the information certifies that the information is complete and accurate.

(ii) Notice to consumer.—If any information that has been deleted from a consumer's file pursuant to subparagraph (A) is reinserted in the file, the consumer reporting agency shall notify the consumer of the reinsertion in writing not later than 5 business days after the reinsertion or, if authorized by the consumer for that purpose, by any other means available to the agency.

(iii) Additional information.—As part of, or in addition to, the notice under clause (ii), a consumer reporting agency shall provide to a consumer in writing not later than 5 business days after the date of the reinsertion—

(I) a statement that the disputed information has been reinserted;

(II) the business name and address of any furnisher of information contacted and the telephone number of such furnisher, if reasonably available, or of any furnisher of information that contacted the consumer reporting agency, in connection with the reinsertion of such information; and

(III) a notice that the consumer has the right to add a statement to the consumer's file disputing the accuracy or completeness of the disputed information.

(C) Procedures to prevent reappearance.—A consumer reporting agency shall maintain reasonable procedures designed to prevent the reappearance in a consumer's file, and in consumer reports on the consumer, of information that is deleted pursuant to this paragraph (other than information that is reinserted in accordance with subparagraph (B)(i)).

(D) Automated reinvestigation system.—Any consumer reporting agency that compiles and maintains files on consumers on a nationwide basis shall implement an automated system through which furnishers of information to that consumer reporting agency may report the results of a reinvestigation that finds incomplete or inaccurate information in a consumer's file to other such consumer reporting agencies.

(6) Notice of results of reinvestigation.—

(A) In general.—A consumer reporting agency shall provide written notice to a consumer of the results of a reinvestigation under this subsection not later than 5 business days after the completion of the reinvestigation, by mail or, if authorized by the consumer for that purpose, by other means available to the agency.

(B) Contents.—As part of, or in addition to, the notice under subparagraph (A), a consumer reporting agency shall provide to a consumer in writing before the expiration of the 5-day period referred to in subparagraph (A)—

(i) a statement that the reinvestigation is completed;
(ii) a consumer report that is based upon the consumer's file as that file is revised as a result of the reinvestigation;

(iii) a notice that, if requested by the consumer, a description of the procedure used to determine the accuracy and completeness of the information shall be provided to the consumer by the agency, including the business name and address of any furnisher of information contacted in connection with such information and the telephone number of such furnisher, if reasonably available;

(iii) a notice that the consumer has the right to add a statement to the consumer's file disputing the accuracy or completeness of the information; and

(iv) a notice that the consumer has the right to request under subsection (d) that the consumer reporting agency furnish notifications under that subsection.

(7) Description of reinvestigation procedure.—A consumer reporting agency shall provide to a consumer a description referred to in paragraph (6)(B)(iii) by not later than 15 days after receiving a request from the consumer for that description.

(8) Expedited dispute resolution.—If a dispute regarding an item of information in a consumer's file at a consumer reporting agency is resolved in accordance with paragraph (5)(A) by the deletion of the disputed information by not later than 3 business days after the date on which the agency receives notice of the dispute from the consumer in accordance with paragraph (1)(A), then the agency shall not be required to comply with paragraphs (2), (6), and (7) with respect to that dispute if the agency—

(A) provides prompt notice of the deletion to the consumer by telephone;

(B) includes in that notice, or in a written notice that accompanies a confirmation and consumer report provided in accordance with subparagraph (C), a statement of the consumer's right to request under subsection (d) that the agency furnish notifications under that subsection; and

(C) provides written confirmation of the deletion and a copy of a consumer report on the consumer that is based on the consumer's file after the deletion, not later than 5 business days after making the deletion.

(b) Statement of dispute

If the reinvestigation does not resolve the dispute, the consumer may file a brief statement setting forth the nature of the dispute. The consumer reporting agency may limit such statements to not more than one hundred words if it provides the consumer with assistance in writing a clear summary of the dispute.

(c) Notification of consumer dispute in subsequent consumer reports
Whenever a statement of a dispute is filed, unless there is reasonable grounds to believe that it is frivolous or irrelevant, the consumer reporting agency shall, in any subsequent consumer report containing the information in question, clearly note that it is disputed by the consumer and provide either the consumer's statement or a clear and accurate codification or summary thereof.

(d) Notification of deletion of disputed information

Following any deletion of information which is found to be inaccurate or whose accuracy can no longer be verified or any notation as to disputed information, the consumer reporting agency shall, at the request of the consumer, furnish notification that the item has been deleted or the statement, codification or summary pursuant to subsection (b) or (c) to any person specifically designated by the consumer who has within two years prior thereto received a consumer report for employment purposes, or within six months prior thereto received a consumer report for any other purpose, which contained the deleted or disputed information.

“”

15 U.S.C. §1681i (emphasis added).

²⁴ New York’s Pattern Jury Instruction Charge (N.Y.P.J.I.) 1:77 which deals with the failure to produce documents states:

“The failure of (plaintiff, defendant) to produce [*state nature of document*] cannot be the basis of an inference against (it, him, her) unless you are satisfied from the evidence in this case that these conditions have been met: first, that there is a document in (its, his, her) possession which relates in an important way to the issue of [*identify issue*] and, second, that (it, he, she) has not offered a reasonable explanation for the failure to produce the document. If these two conditions are met, you may, in weighing the evidence, although you are not required to, infer that the document if produced would not have supported (plaintiff, defendant) on that question [*if opposing side introduced evidence on the issue*] and would not contradict the evidence offered by (plaintiff, defendant) on that question, and you may, although you are not required to, draw the strongest inference against the (plaintiff, defendant) on that question which the opposing evidence permits.”

N.Y. P.J.I. 1:77.

²⁵ **15 U.S.C. §1681n. Civil liability for willful noncompliance**

“(a) In general. Any person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of—

(1) (A) any actual damages sustained by the consumer as a result of the failure or damages of not less than \$ 100 and not more than \$ 1,000; or

(B) in the case of liability of a natural person for obtaining a consumer report under false pretenses or knowingly without a permissible purpose, actual damages sustained by the consumer as a result of the failure or \$ 1,000, whichever is greater;

(2) such amount of punitive damages as the court may allow; and

(3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney’s fees as determined by the court.

(b) Civil liability for knowing noncompliance

Any person who obtains a consumer report from a consumer reporting agency under false pretenses or knowingly without a permissible purpose shall be liable to the consumer reporting agency for actual damages sustained by the consumer reporting agency or \$1,000, whichever is greater.

(c) Attorney's fees

Upon a finding by the court that an unsuccessful pleading, motion, or other paper filed in connection with an action under this section was filed in bad faith or for purposes of harassment, the court shall award to the prevailing party attorney's fees reasonable in relation to the work expended in responding to the pleading, motion, or other paper.”

15 U.S.C. §1681n.

²⁶ **15 U.S.C. §1681o. Civil liability for negligent noncompliance**

“(a) In general

Any person who is negligent in failing to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of—

(1) any actual damages sustained by the consumer as a result of the failure; and

(2) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

(b) Attorney's fees

On a finding by the court that an unsuccessful pleading, motion, or other paper filed in connection with an action under this section was filed in bad faith or for purposes of harassment, the court shall award to the prevailing party attorney's fees reasonable in relation to the work expended in responding to the pleading, motion, or other paper.”

15 U.S.C. §1681o.

²⁷ 15 U.S.C. §1681g(c)(2)(E) states, in pertinent part that “[a] consumer reporting agency shall provide to a consumer . . . a statement that a consumer reporting agency is not required to remove accurate derogatory information from the file of a consumer, unless the information is outdated . . . or **cannot be verified.**” 15 U.S.C. §1681g(c)(2)(E) (emphasis added).

²⁸ Pursuant to federal law, social security numbers are confidential. 42 U.S.C. §405(c)(2)(c)(viii)(I).

“Social security account numbers and related records that are obtained or maintained by **authorized persons** pursuant to any provision of law . . . shall be confidential, and no authorized person shall disclose any such social security account number or related record.”

42 U.S.C. §405(c)(2)(c)(viii)(I) (emphasis added). An authorized person, under that federal statute, has been defined to include

“ . . . an officer or employee of the United States, an officer or employee of any State, political subdivision of a State, or agency of a State or political subdivision of a State, **and any other person (or officer or employee thereof), who has or had access to social security account numbers or related records pursuant to any provision of law** For purposes of this subclause, the term “officer or employee” includes a former officer or employee.”

42 U.S.C. §405(c)(2)(c)(viii)(III). *See also Meyerson v. Prime Realty Svcs., LLC*, 7 Misc.3d 911, 796 N.Y.S.2d 848 (Sup. Ct. New York County 2005)(as between two private parties in a landlord-tenant transaction, landlord may not demand confidential social security number, which is deemed privileged, from tenant under law that does not so provide or landlord will risk being liable for money damages under deceptive business practice act, N.Y. Gen'l Bus. L. §349).

²⁹ **15 U.S.C. §1681e. Compliance procedures**

“(a) Identity and purposes of credit users

Every consumer reporting agency shall maintain reasonable procedures designed to avoid violations of [section 1681c](#) of this title and to limit the furnishing of consumer reports to the purposes listed under [section 1681b](#) of this title. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Every consumer reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report. No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a purpose listed in [section 1681b](#) of this title.

(b) Accuracy of report

Whenever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.”

³⁰ **§ 1681p. Jurisdiction of courts; limitation of actions**

“An action to enforce any liability created under this subchapter may be brought in any appropriate United States district court, without regard to the amount in controversy, or in any other court of competent jurisdiction, not later than the earlier of—

(1) 2 years after the date of discovery by the plaintiff of the violation that is the basis for such liability; or

(2) 5 years after the date on which the violation that is the basis for such liability occurs.”

³¹ **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—

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation by the individual in any process provided for by this subpart, including the filing of a complaint under this section; and

(2) Must refrain from intimidation and retaliation as provided in §160.316 of this subchapter.

(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.
- (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)."

45 C.F.R. §164.530.

Banks also have their 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).

³² N.Y. Technology Law § 208.

"Notification; person without valid authorization has acquired private information"

1. As used in this section, the following terms shall have the following meanings:

(a) "Private information" shall mean personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- (1) social security number;
- (2) driver's license number or non-driver identification card number; or
- (3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(b) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such state entity may consider the following factors, among others:

- (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
- (2) indications that the information has been downloaded or copied; or
- (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(c) "State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except:

- (1) the judiciary; and
 - (2) all cities, counties, municipalities, villages, towns, and other local agencies.
- (d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues,

or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification under subdivision two of this section.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The state entity shall consult with the state office of cyber security and critical infrastructure coordination to determine the scope of the breach and restoration measures.

3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the state entity who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

(c) telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons; or

(d) Substitute notice, if a state entity demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such state entity has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; and

(3) notification to major statewide media.

6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

7. (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the consumer protection board, and the state office of

cyber security and critical infrastructure coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

8. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.”

³³ N.Y. Gen'l Bus. Law §899-aa.

“Notification; person without valid authorization has acquired private information

1. As used in this section, the following terms shall have the following meanings:

(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

(b) "Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:

- (1) social security number;
- (2) driver's license number or non-driver identification card number; or
- (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

(c) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.

Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

- (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
- (2) indications that the information has been downloaded or copied; or
- (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section.

2. Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any

breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

3. Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.

(c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or

(d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such business has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and

(3) notification to major statewide media.

6. (a) whenever the attorney general shall believe from evidence satisfactory to him that there is a violation of this article he may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to ten dollars per instance of failed notification, provided that the latter amount shall not exceed one hundred fifty thousand dollars.

(b) the remedies provided by this section shall be in addition to any other lawful remedy available.

(c) no action may be brought under the provisions of this section unless such action is commenced within two years immediately after the date of the act complained of or the date of discovery of such act.

7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification and a description of

the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

8. (a) In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

9. The provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.”

³⁴ **15 U.S.C. §1681h(e). Limitation of liability**

“Except as provided in [sections 1681n](#) and [1681o](#) of this title, no consumer may bring any action or proceeding in the nature of defamation, invasion of privacy, or negligence with respect to the reporting of information against any consumer reporting agency, any user of information, or any person who furnishes information to a consumer reporting agency, based on information disclosed pursuant to [section 1681g](#), 1681h, or [1681m](#) of this title, or based on information disclosed by a user of a consumer report to or for a consumer against whom the user has taken adverse action, based in whole or in part on the report except as to false information furnished with malice or willful intent to injure such consumer.”

15 U.S.C. §1681h(e).

³⁵ **18 U.S.C. §1961. RICO Definitions**

As used in this chapter [18 USCS §§ 1961 *et seq.*]—

(1) "racketeering activity" means (A) any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or dealing in a controlled substance or listed chemical (as defined in section 102 of the Controlled Substances Act), which is chargeable under State law and punishable by imprisonment for more than one year; (B) any act which is indictable under any of the following provisions of title 18, United States Code: Section 201 (relating to bribery), section 224 (relating to sports bribery), sections 471, 472, and 473 (relating to counterfeiting), section 659 (relating to theft from interstate shipment) if

the act indictable under section 659 is felonious, section 664 (relating to embezzlement from pension and welfare funds), sections 891-894 (relating to extortionate credit transactions), **section 1028 (relating to fraud and related activity in connection with identification documents)**, **section 1029 (relating to fraud and related activity in connection with access devices)**, section 1084 (relating to the transmission of gambling information), section 1341 (relating to mail fraud), section 1343 (relating to wire fraud), section 1344 (relating to financial institution fraud), section 1425 (relating to the procurement of citizenship or naturalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), sections 1461-1465 (relating to obscene matter), section 1503 (relating to obstruction of justice), section 1510 (relating to obstruction of criminal investigations), section 1511 (relating to the obstruction of State or local law enforcement), section 1512 (relating to tampering with a witness, victim, or an informant),

section 1513 (relating to retaliating against a witness, victim, or an informant), section 1542 (relating to false statement in application and use of passport), section 1543 (relating to forgery or false use of passport), section 1544 (relating to misuse of passport), section 1546 (relating to fraud and misuse of visas, permits, and other documents), sections 1581-1592 (relating to peonage, slavery, and trafficking in persons), section 1951 (relating to interference with commerce, robbery, or extortion), section 1952 (relating to racketeering), section 1953 (relating to interstate transportation of wagering paraphernalia), section 1954 (relating to unlawful welfare fund payments), section 1955 (relating to the prohibition of illegal gambling businesses), section 1956 (relating to the laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 1958 (relating to use of interstate commerce facilities in the commission of murder-for-hire), section 1960 (relating to illegal money transmitters), sections 2251, 2251A, 2252, and 2260 (relating to sexual exploitation of children), sections 2312 and 2313 (relating to interstate transportation of stolen motor vehicles), sections 2314 and 2315 (relating to interstate transportation of stolen property), section 2318 (relating to trafficking in counterfeit labels for phonorecords, computer programs or computer program documentation or packaging and copies of motion pictures or other audiovisual works), section 2319 (relating to criminal infringement of a copyright), section 2319A (relating to unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances), section 2320 (relating to trafficking in goods or services bearing counterfeit marks), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), sections 2341-2346 (relating to trafficking in contraband cigarettes), sections 2421-24 (relating to white slave traffic), sections 175-178 (relating to biological weapons), sections 229-229F (relating to chemical weapons), section 831 (relating to nuclear materials), (C) any act which is indictable under title 29, United States Code, section 186 (dealing with restrictions on payments and loans to labor organizations) or section 501(c) (relating to embezzlement from union funds), (D) any offense involving fraud connected with a case under title 11 (except a case under section 157 of this title), fraud in the sale of securities, or the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in a controlled substance or listed chemical (as defined in section 102 of the Controlled Substances Act), punishable under any law of the United States, (E) any act which is indictable under the Currency and Foreign Transactions Reporting Act, (F) any act which is indictable under the Immigration and Nationality Act, section 274 (relating to bringing in and harboring certain aliens), section 277 (relating to aiding or assisting certain aliens to enter the United States), or section 278 (relating to importation of alien for immoral purpose) if the act indictable under such section of such Act was committed for the purpose of financial gain, or (G) any act that is indictable under any provision listed in section 2332b(g)(5)(B);

(2) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, any territory or possession of the United States, any political subdivision, or any department, agency, or instrumentality thereof;

(3) "person" includes any individual or entity capable of holding a legal or beneficial interest in property;

(4) "enterprise" includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity;

(5) "pattern of racketeering activity" requires at least two acts of racketeering activity, one of which occurred after the effective date of this chapter and the last of which occurred within ten years (excluding any period of imprisonment) after the commission of a prior act of racketeering activity;

(6) "unlawful debt" means a debt (A) incurred or contracted in gambling activity which was in violation of the law of the United States, a State or political subdivision thereof, or which is unenforceable under State or Federal law in whole or in part as to principal or interest because of the laws

relating to usury, and (B) which was incurred in connection with the business of gambling in violation of the law of the United States, a State or political subdivision thereof, or the business of lending money or a thing of value at a rate usurious under State or Federal law, where the usurious rate is at least twice the enforceable rate;

(7) "racketeering investigator" means any attorney or investigator so designated by the Attorney General and charged with the duty of enforcing or carrying into effect this chapter;

(8) "racketeering investigation" means any inquiry conducted by any racketeering investigator for the purpose of ascertaining whether any person has been involved in any violation of this chapter or of any final order, judgment, or decree of any court of the United States, duly entered in any case or proceeding arising under this chapter;

(9) "documentary material" includes any book, paper, document, record, recording, or other material; and

(10) "Attorney General" includes the Attorney General of the United States, the Deputy Attorney General of the United States, the Associate Attorney General of the United States, any Assistant Attorney General of the United States, or any employee of the Department of Justice or any employee of any department or agency of the United States so designated by the Attorney General to carry out

the powers conferred on the Attorney General by this chapter. Any department or agency so designated may use in investigations authorized by this chapter either the investigative provisions of this chapter or the investigative power of such department or agency otherwise conferred by law."

18 U.S.C. §1961(emphasis added).

³⁶ **18 U.S.C. §1962. Prohibited RICO activities**

"(a) It shall be unlawful for any person who has received any income derived, directly or indirectly, from a pattern of racketeering activity or through collection of an unlawful debt in which such person has participated as a principal within the meaning of section 2, title 18, United States Code [18 USCS § 2], to use or invest, directly or indirectly, any part of such income, or the proceeds of such income, in acquisition of any interest in, or the establishment or operation of, any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce. A purchase of securities on the open market for purposes of investment, and without the intention of controlling or participating in the control of the issuer, or of assisting another to do so, shall not be unlawful under this subsection if the securities of the issuer held by the purchaser, the members of his immediate family, and his or their accomplices in any pattern or racketeering activity or the collection of an unlawful debt after such purchase do not amount in the aggregate to one percent of the outstanding securities of any one class, and do not confer, either in law or in fact, the power to elect one or more directors of the issuer.

(b) It shall be unlawful for any person through a pattern of racketeering activity or through collection of an unlawful debt to acquire or maintain, directly or indirectly, any interest in or control of any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce.

(c) It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity or collection of unlawful debt.

(d) It shall be unlawful for any person to conspire to violate any of the provisions of subsection (a), (b), or (c) of this section."

18 U.S.C. §1962 (emphasis added).