

### COUNCIL ON JUDICIAL ADMINISTRATION

JAY G. SAFER
Chair
3 World Financial Center
NEW YORK, NY 10281
Phone: (212) 812-8305
Fax: (212) 812-8365
JSafer@lockelord.com

DAVID I. WAX SECRETARY 3 WORLD FINANCIAL CENTER NEW YORK, NY 10281 Phone: (212) 812-8326 Fax: (212) 812-8396 dwax@lockelord.com

> The Honorable Jonathan Lippman Chief Judge of the New York State Court of Appeals Court of Appeals Hall 20 Eagle Street Albany, NY 12207-1095

> The Honorable Ann T. Pfau Chief Administrative Judge of the State of New York Office of Court Administration 25 Beaver Street New York, NY 10004

Dear Chief Judge Lippman and Chief Administrative Judge Pfau:

The Council on Judicial Administration of the New York City Bar Association is pleased to transmit for your consideration the attached report and proposed rule on what we believe to be an important and timely subject - the need to protect sensitive personal information (such as social security numbers) from unnecessary disclosure in court records and guarding against the attendant danger of identity theft.

As the report notes, there is currently no Statewide rule protecting sensitive personal information in the New York courts. The federal courts have such a rule as do many other states. Now that court filings are increasingly available on the internet or otherwise distributed in electronic form, we believe it is important to promulgate an appropriate rule at the earliest possible time. We hope our report and proposed rule we propose on behalf of the Association will assist in accomplishing this needed action.



We stand ready to assist in any way we can with this matter and would be pleased to discuss it with you at your convenience.

Yours very truly,

Jos a toke

Jay G. Safer

Chair of the Council on Judicial Administration

cc:

Ron Youkins

John W. McConnell Alan Rothstein Steven M. Kayman

Enclosures

### REPORT RECOMMENDING A NEW YORK STATE COURT RULE REQUIRING THAT SENSITIVE PERSONAL INFORMATION BE OMITTED OR REDACTED FROM DOCUMENTS FILED WITH CIVIL COURTS

Subcommittee on Electronic Court Records Steven M. Kayman, Chair

Council on Judicial Administration Jay G. Safer, Chair

**Submitted February 2, 2010** 

The members of the Subcommittee on Electronic Records are:

- Jeremy Feinberg
- Steven M. Kayman
- Paul H. Levinson
- Hon. Andrea Masley
- Karen Milton
- Hon. Jacqueline W. Silbermann (Ret.)

The Subcommittee would like to thank the following people for their assistance with this Report:

- Justin F. Heinrich, Proskauer Rose LLP, who served superbly as secretary to the Subcommittee and played a major role in drafting the Report; and
- Summer Associates Tiffany Compres, Proskauer Rose LLP, and Meghan Mulderig, McLaughlin & Stern, LLP, for their excellent research support.

### TABLE OF CONTENTS

		Page
I.	Introduction	1
II.	There Is No Law or Uniform Court Rule Protecting Sensitive Personal Information in the New York State Courts	3
III.	Protection of Sensitive Personal Information in Other Jurisdictions	6
IV.	The Proposed Rule	9
V.	Further Recommendations	11
Appen	ndix A (Proposed Rule)	13

### I. INTRODUCTION

The Council on Judicial Administration of the Association of Bar of the City of New York established the Subcommittee on Electronic Court Records to consider the challenge of how to protect the privacy and confidentiality of sensitive personal information as court records become increasingly available electronically. Over the course of the past year and a half, the Subcommittee has met and conferred and researched the issue and respectfully submits this Report recommending the adoption of a new rule applicable to all documents filed (electronically or in hard copy) in all New York State civil courts.

Documents filed with civil courts have presumptively been public records in New York and in the United States generally, accessible to anyone willing to make the trip to a courthouse. Recently, however, New York's Unified Court System ("UCS") has made it a goal (and, indeed, a laudable one) to post court documents on the Internet and therefore make them available to anyone with a computer and Internet connection. Press Release, UCS, "New York Court Records to be Posted on the Internet" (February 25, 2004) (available at www.courts.state.ny.us/press/pr2004\_21.shtml). Private companies, such as Courthouse News Service, also make court records available to subscribers and the general public. As a result, it is becoming easier and easier for the general public to access court records.

Beyond providing easier access, the posting of court documents on the Internet poses the unique problem of permanency. While a paper document housed in a courthouse file may be removed or amended if sensitive information is unnecessarily disclosed or if an error is discovered, once a document is digitized and published on the Internet, that digital copy may continue to exist on the Internet, even if it is subsequently removed or amended from the court's

The subject of this report is sensitive personal information belonging to individuals (such as social security numbers), not confidential business information. The Subcommittee believes, however, that consideration should be given to extending at least some of the protections of the Proposed Rule to business enterprises. For example, public dissemination of a company's bank account number could pose a risk of identity theft that is not so different from what an individual would face.

records. For example, once a document is posted on the Internet, a footprint of it may remain on the Internet even if the online service "removes" the record. Internet services such as the "waybackmachine" (available at www.archive.org) allow Internet users to access the historical content of Internet websites. Additionally, an individual who accessed the document before it was removed or amended may have downloaded it and posted it on another website, such as a weblog.<sup>2</sup> Thus, the removal of a digitized document from the court's or an online service's website does not necessarily have the same effect as removing a paper document from a courthouse.

These two developments – easier accessibility and potential permanence – have led to increased concern about the disclosure of sensitive personal information in court filings. The reality is that the notion of privacy of court records is a misnomer. Once something is filed, absent a court order sealing a record, there is no such thing as privacy. Concerns about "identity theft," an increasingly common phenomenon, have also helped focus attention on protecting private information from disclosure in court filings. Social security numbers and financial account numbers are perhaps the two most obvious categories of sensitive personal information – though there are others, as discussed below.

Many jurisdictions, including the federal courts and at least fifteen states, have passed legislation or issued rules to help protect sensitive personal information from unnecessary

A "weblog" (or "blog" for short) is defined as "a personal Web site that provides updated headlines and news articles of other sites that are of interest to the user [and] also may include journal entries, commentaries and recommendations compiled by the user." Webster's New Millennium Dictionary of English, Preview Ed. (v.0.9.7) (available at www. dictionary.com).

Of course, even in situations where there is a court order to seal a case file or particular record, inadvertent disclosure of sensitive personal information may still occur, for instance, as a result of human error.

The Federal Trade Commission estimates that approximately 9 million Americans have their identities stolen each year. Federal Trade Commission Identity Theft Page, www.ftc.gov/bcp/edu/microsites/idtheft (last visited April 13, 2009).

disclosure in court filings.<sup>5</sup> The Subcommittee recommends a court rule for all New York civil courts. Among other goals, the Subcommittee hopes such a rule will help raise the consciousness of persons filing papers with New York courts about the need to protect sensitive personal information.

# II. THERE IS NO LAW OR UNIFORM COURT RULE PROTECTING SENSITIVE PERSONAL INFORMATION IN THE NEW YORK STATE COURTS

There is currently no law or uniform New York State court rule addressing the protection of sensitive personal information in documents filed with the courts. Although some individual courts have sought to protect certain types of information, the Subcommittee respectfully submits that there should be a uniform State-wide rule and recommends the adoption of the proposed court rule (the "Proposed Rule") attached hereto as Appendix A.<sup>6</sup>

Several years ago, some initial steps were taken toward the promulgation of such a rule. In April 2002, then Chief Judge Judith S. Kaye formed the Commission on Public Access to Court Records (the "Commission") which was "charged with examining the sometimes competing interests of privacy and open access relating to information in court case files." Press Release, UCS, "Commission to Examine Future of Court Documents on the Internet" (April 24,

At least two states have also enacted laws to protect sensitive personal information that is transmitted in the course of consumer transactions. Thus, Massachusetts and Nevada require businesses to encrypt their customers' personal information if that information is electronically transmitted. Nev. Rev. Stat. § 597.970 (2007); Mass. Gen. Laws ch. 93H § 2 (2007); 201 Mass. Code Regs. 17.00 (2009). Effective January 1, 2010, Nevada's current consumer data protection law, Nev. Rev. Stat. § 597.970, was replaced by a new law which requires encryption of personal information not only if that information is electronically transmitted but also if the personal information leaves the "logical or physical controls of the data collector," including data on a "data storage device." S.B. 227, 2009 Leg. 75th Sess. (Nev. 2009) (enacted).

The Subcommittee considered recommending application of the Proposed Rule to criminal as well as civil cases. However, after substantial discussion and input from outside the Subcommittee, it was decided to recommend limiting the Proposed Rule's applicability to civil actions. The Subcommittee's reasoning is that the two principal issues of concern (the accessibility and permanence of court records) appear not to apply to criminal court records, which are not presently posted on the Internet. In addition, the Subcommittee understands that there may be situations in which some of the proposed protected sensitive personal information must be included in criminal court filings, which would make adherence to the Proposed Rule difficult. We recommend further consideration of whether and, if so, how to protect sensitive personal information from being disclosed in criminal court filings.

2002) (available at www.nycourts.gov/press/pr2002\_07.shtml). The Commission's primary objective was to determine whether any restrictions should be placed on court documents that are made available on the Internet (via the UCS) but are otherwise publicly available in paper form at courthouses.

The Commission, chaired by attorney Floyd Abrams, published a report in February 2004 favoring full disclosure and made several recommendations with respect to the availability of court documents on the Internet. A copy of the full report is available at www.courts...//. One of the Commission's recommendations was that, without leave of the court, the following information should not be included in full in any paper or electronic documents filed with the court: social security numbers, financial account numbers, names of minor children and full birth dates of any individual.

Over five years later, however, there is still no State-wide rule aimed at preventing an individual's sensitive personal information from being included in public filings with New York courts.

Some individual courts and court administrators have taken it upon themselves to issue local rules and guidelines protecting sensitive personal information but such piecemeal efforts, although commendable, do not obviate the need for a State-wide rule.

For example, on February 2, 2006, then Chief Administrative Judge Jonathan Lippman issued a memorandum to all New York judges, recommending that certain personal identifying information be redacted from judicial decisions, in light of the availability of court decisions on the Internet. Attached to Judge Lippman's memorandum was a memorandum from Michael Colodner, Counsel for the Office of Court Administration, dated January 26, 2005, which set forth guidelines for judges to prevent sensitive personal information from appearing in decisions. Specifically, Mr. Colodner recommended that the names of minor children, and numerical

identifiers such as social security numbers, birth dates, driver's license numbers, and bank, credit and financial account numbers be redacted from judicial decisions. *Id*.

In addition, effective September 15, 2006, the Civil Division of New York County

Supreme Court adopted a rule related to the exclusion of sensitive personal information in

documents filed with the court – in contemplation of increased public access to court documents
via the "Supreme Court Records On Line Library ("SCROLL").<sup>7</sup> Notice to the Bar and Rules

(Updated) – Project on Public Access to Court Records (Case Documents On-Line), UCS, First

Judicial District, Supreme Court, Civil Branch (Sept. 7, 2006) (available at http://www.nycourts.

gov/supctmanh/news\_&\_announcements.htm). The rule states that, for documents filed with the
court and posted on SCROLL, attorneys should

not set out in such documents social security numbers, bank account numbers, and the names of minor children, dates of birth, health information concerning any individual and other similar sensitive information, or, if doing so is unavoidable, shall, to the extent practical, provide only a portion of the information (e.g., some but not all digits of an account number, initials only in place of the names of minor children).

Id.

Since late 2007, the Civil Court of the City of New York has required persons who file documents "that contain social security numbers or derivatives of those numbers" to "redact the numbers before filing the papers with the court." Chief Clerk Memorandum-172, Civil Court of the City of New York (Oct. 23, 2007) (available at www.nycourts.gov/courts/nyc/civil/directives/CCM/ccm172.pdf). If a court record contains such information, "the clerk is to promptly redact this information from the record." *Id*.

Individual judges have also attempted to prevent the unnecessary disclosure of sensitive personal information in court filings. See, e.g., 1/7/2010 N.Y.L.J. 1, col. 1 (reporting ruling by

SCROLL is a free on-line public service offered by the UCS through which the general public may electronically access records filed with the court by entering an index number or party name. The service is available at http://iapps.courts.state.ny.us/iscroll/index.jsp.

Nassau County Supreme Court Justice F. Dana Winslow refusing to accept any document containing a social security number because of the danger of making private information publicly accessible).

In addition to the protection for sensitive personal information that the Proposed Rule offers the public, the Proposed Rule would achieve uniformity among New York courts with respect to the protection of sensitive personal information. It will obviate the need for the present judicial piecemeal approach. The Proposed Rule will also eliminate the potential for confusion among those who file papers with different courts. Thus, because the Proposed Rule would be uniform for all non-criminal New York courts, an individual filing a document with a court will not have to worry that certain information does or does not have to be removed because of that court's individual rules. The Proposed Rule would also apply to all documents which are filed, whether in hard copy or electronic form.

# III. PROTECTION OF SENSITIVE PERSONAL INFORMATION IN OTHER JURISDICTIONS

During the course of its research, the Subcommittee identified statutes and rules of other jurisdictions that address the protection of sensitive personal information in documents filed with the courts. Although there is no uniformity among jurisdictions, several general approaches have been taken, which are described below.

The Federal Rules of Civil Procedure provide that someone filing papers who wishes to include "an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial account number" in an electronic or paper filing with the court, must redact portions of that information. F.R.C.P. 5.2(a).<sup>8</sup>
Although Federal Rule 5.2 is limited to five general types of sensitive personal information, the

Federal Rule 5.2 was adopted in 2007 in response to the Report on the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files (the "Rule 5.2 Report"), originally filed in September 2001 and amended in December 2006. The Rule 5.2 Report is available at www.privacy.uscourts.gov/Policy.htm.

Advisory Committee Notes suggest that "[i]t may also be necessary to protect information not covered by the redaction requirement – such as driver's license numbers and alien registration numbers – in a particular case. In such cases, protection may be sought under subdivision (d)<sup>9</sup> or (e)."<sup>10</sup>

At least fifteen states have enacted laws or rules regarding the exclusion of or limiting public access to sensitive personal information in filings with the court. Some states, such as Alaska and Minnesota, simply limit public access to electronic documents that do not contain certain sensitive personal information. *See* Alaska Admin. Rule 37.8; Minn. Rules of Public Access to Records of the Judicial Branch, Rule 8(2)(b). Other states prohibit public access to all documents (paper or electronic) containing certain sensitive personal information. *See*, *e.g.*, Ark. Admin. Order 19, § 7(A)(4), (5), (8).

The Subcommittee believes that the rules of these states may create confusion with respect to what can or cannot be posted on the Internet. Further, such rules would not protect sensitive personal information from being disclosed if someone went to the courthouse to look at the paper document or if a document inadvertently was posted on the Internet. Additionally, the rules of these states appear to place significant burdens on court personnel to ensure that documents do not contain sensitive personal information before posting them to the Internet or otherwise allowing the public to access them. The Subcommittee believes that, at least in New York, the volume of filings makes it unrealistic to expect court personnel to do the job and that responsibility should therefore lie with attorneys and other persons filing documents.

Federal Rule 5.2(d) provides that "The court may order that a filing be made under seal without redaction. The court may later unseal the filing or order the person who made the filing to file a redacted version for the public record."

Federal Rule 5.2(e) provides that "For good cause, the court may by order in a case: (1) require redaction of additional information; or (2) limit or prohibit a nonparty's remote electronic access to a document filed with the court."

Other states prohibit certain sensitive personal information from being included in court documents. For instance, Kansas requires the omission of social security numbers, dates of birth and financial account numbers from papers filed with the court unless such information must be included (for social security number and date of birth) or is relevant (for financial account information), in which case the information must be partially redacted. Kan. Sup. Ct. Rule 123. California Court Rule 1.20(b)(2) states in part that "parties and their attorneys must not include, or must redact where inclusion is necessary, [social security numbers and financial account numbers] from all pleadings and other papers filed in the court's public file, whether filed in paper or electronic form, unless otherwise provided by law or ordered by the court." Similarly, Washington General Rule 31(e)(1) requires that "parties shall not include, and if present shall redact [Social Security numbers, financial account numbers and driver's license numbers] from all documents filed with the court, whether filed electronically or in paper, unless necessary or otherwise ordered by the Court."

The Subcommittee believes that State and federal rules such as these fail to safeguard some categories of information which should be protected and do not create a clear enough presumption against including sensitive personal information in filings unless truly necessary. Some of the rules are also less than clear about what should be redacted.

Other states *require* the omission or redaction of certain sensitive personal information while *allowing* the omission or redaction of other sensitive personal information. For instance, Rule 1.422 of Iowa's Court Rules requires the omission or redaction of social security numbers, financial account numbers, personal identification numbers and "other unique identifiers" from documents or exhibits filed with the court. Specifically, the Iowa rule requires the omission of the information unless the "information is material to the proceedings or disclosure is otherwise required by law," in which case the information must be partially redacted. The Iowa rule also allows the omission or redaction of certain other information, such as personal identifying

numbers (e.g., driver's license numbers), medical information, employment history, personal financial information, proprietary or trade secret information, information concerning a person's cooperation with the government, information concerning crime victims, sensitive security information, home addresses, dates of birth, and names of minor children.<sup>11</sup>

#### IV. THE PROPOSED RULE

The Proposed Rule is meant to protect individual members of the public from the disclosure of their sensitive personal information in court documents, unless there is a demonstrable need to include such information. The Subcommittee believes that the Proposed Rule will achieve this goal and will do so more effectively and comprehensively than the rules of other jurisdictions.

The Proposed Rule differs significantly from the protections other jurisdictions have in place. First, the Proposed Rule offers greater protection for sensitive personal information than most jurisdictions. While some jurisdictions only protect a couple of categories of information (e.g., social security numbers and financial account information), the Proposed Rule enumerates nine categories of information which should not be included in documents filed with the court. Additionally, the Proposed Rule begins with the presumption that the sensitive personal information should not be included in court filings at all, even in redacted form. Only in certain circumstances may the nine proscribed categories of information be included, and even then, only in partially redacted form. Other jurisdictions allow the inclusion of the partially redacted sensitive personal information without any good cause requirement.

Subsection (a) of the Proposed Rule states its purpose. First, the Proposed Rule is intended to limit the potential for the illicit theft of an individual's identity through information

The Subcommittee considered including in the Proposed Rule a subsection similar to Iowa's rule, suggesting, but not requiring, that certain information be omitted or redacted from court filings – such as medical and financial information, home and cellular phone numbers and email addresses. After extensive discussion and input from others, however, the Subcommittee decided that a simpler rule, which could be more readily implemented and more easily understood, would better serve, at least in the first instance.

obtained from papers filed with the court. In addition, the Proposed Rule seeks to prevent parties in a court proceeding from unnecessarily disclosing sensitive personal information as an abusive litigation tactic.<sup>12</sup>

Subsection (b)(1) describes the nine categories of sensitive personal information that, absent compelling reasons, must be removed entirely from documents (including attachments) filed with the courts. The Subcommittee recognizes that its Proposed Rule offers more protection than Federal Rule 5.2 in that it mandates the omission of the entirety of certain sensitive personal information, as opposed to allowing, for example, partial social security numbers. The Subcommittee feels there are very limited circumstances under which the inclusion of **any** of the sensitive personal information listed in (b)(1) in a court document is necessary to a legal proceeding. Even an abbreviated version of the sensitive personal information contains elements of the entire information. For instance, access to the last four digits of a social security number places someone intent on stealing another's identity 4/9 closer to obtaining the full number. The better practice, and the one mandated by the Proposed Rule, is to not include any sensitive personal information in filings without a compelling reason. The Proposed Rule also offers protection to a broader variety of sensitive personal information than does the Federal Rule.

The Proposed Rule begins with the basic presumption that certain forms of information should not be included in documents filed with the court. The Subcommittee recognizes, however, that filers may have a need in particular cases to disclose some of the sensitive personal information identified in (b)(1). In situations where the person filing a document has a good faith basis to believe that the sensitive personal information described in (b)(1) is material or

It is the Subcommittee's belief that sensitive personal information is most often disclosed in filings, not out of malice but inadvertently, out of thoughtlessness. Again, that is why a major goal of the Proposed Rule is consciousness-raising.

necessary to the action and that there are compelling reasons to include the information in the filing, subsection (b)(2) permits redacted versions of the information to be included.

Subsection (c) places the obligation to ensure compliance with the Proposed Rule on the person making the filing and not on the clerks of the court.

Subsection (d) exempts from the Proposed Rule any document filed in its entirety under seal. Filers should not take this as an opportunity, however, to refrain from a review of documents being filed to exclude sensitive personal information whenever possible. There are situations, for example, in which documents filed under seal are subsequently unsealed.

Flexibility in the Proposed Rule can be found in subsection (e), which allows a New York State court to "vary the provisions of this [Proposed] Rule as justice and sound case administration may make appropriate" – for good cause shown. The Subcommittee recognizes that every case is different; and there may be circumstances, however rare, in which the protections of the Proposed Rule need to be modified in order to meet the needs of that particular case.

### V. FURTHER RECOMMENDATIONS

It is the Subcommittee's hope that the Proposed Rule, once in effect, will raise the consciousness of attorneys, pro se litigants and others filing papers about the need to safeguard sensitive personal information from unnecessary disclosure.<sup>13</sup>

To publicize the adoption of the Proposed Rule, and serve as a safeguard against thoughtless filings, the Subcommittee recommends the prominent display of a poster in New

The Subcommittee discussed the possibility of proposing an ethical rule in combination with the Proposed Rule to further reinforce the importance of the protection of sensitive personal information and increase awareness among court filers. It appears that no other jurisdiction has such an ethical rule, so we would be breaking new ground. The Subcommittee decided not to recommend an ethical rule at this time, in part, because the failure to comply with a court rule can already be considered a violation of the New York Rules of Professional Conduct. See N.Y. Rules of Prof. Conduct, Rule 3.4(c) ("A lawyer shall not disregard... a standing rule of a tribunal."). In addition, the Subcommittee felt that a proposed ethical rule would likely be controversial and did not want to risk slowing the adoption of a needed court rule by proposing what might be a less necessary and more controversial ethical rule. Depending on future developments, including the implementation of and compliance with the Proposed Rule, the Subcommittee believes an ethical rule might warrant further consideration.

York State court filing offices. Additionally, for documents electronically filed with courts, the Subcommittee recommends an electronic message or display that a filer would be required to check or click on to acknowledge that he or she is in compliance with the Proposed Rule. Continued display of the poster and electronic filing acknowledgement will educate first-time filers and reinforce the requirements of the Proposed Rule to seasoned filers. The Subcommittee would be happy to work with the Office of Court Administration in designing such a poster and electronic filing acknowledgment.

Recognizing the novel nature of the Proposed Rule and the relative infancy of other rules in effect in other jurisdictions, the Subcommittee also recommends the formation of a Statewide, court system-sponsored committee tasked with the duty of evaluating the implementation of the Proposed Rule and formulating a report within two years after the Proposed Rule's promulgation. The committee would report on compliance with the Proposed Rule as well as possible suggestions, if any, for amendment.

#### APPENDIX A

## PROPOSED COURT RULE – PROTECTION OF SENSITIVE PERSONAL INFORMATION

- (a) Statement of Purpose The purpose of this Rule is to limit the potential, through the unnecessary disclosure of sensitive personal information in civil court filings, for the theft of an individual's identity. The Rule is also intended to prevent the unnecessary disclosure of an individual's sensitive personal information in civil court filings as an abusive litigation tactic.
- (b) (1) Unless otherwise authorized by court order or law, and subject to the next subsection of this Rule, the following sensitive personal information of an individual **must** be omitted or redacted from any paper or electronic document filed with any New York State civil court, including exhibits or attachments thereto: (i) social security numbers, (ii) taxpayer identification numbers of a natural person, (iii) bank and other financial account numbers, (iv) passport numbers, (v) driver's license numbers, (vi) government issued identification numbers, (vii) other identification numbers which uniquely identify an individual; (viii) the names of minor children; and (ix) dates of birth.
- (2) When a person filing a document believes in good faith that the inclusion of the sensitive personal information described in (b)(1) is material or necessary to the action **and** that there are compelling reasons to include the sensitive information in the filing, then only the following information may be included: the last four digits of any of the numbers described in (i) (vi); no more than half of the numbers of (vii); the initials of minor children; and an individual's year of birth.
- (c) It is the sole responsibility of the person making the filing to ensure compliance with this Rule.
- (d) This Rule does not apply to any document that by court order or by operation of law is filed in its entirety under seal.
- (e) A New York State court may, for good cause shown, vary the provisions of this Rule as justice and sound case administration may make appropriate.
- (f) This Rule is effective as of \_\_\_\_\_. There is no obligation, under this Rule, to amend or correct any filing made prior to the effective date.