Clerk's News 2016

October 14, 2016 **Editors: Diann Freeman and Dina Ventura**

In This Issue:

Notice Regarding Recall Status of Hon. Robert E. Littlefield, Jr.

By: Hon. Margaret Cangilos-Ruiz

I am happy to report that notwithstanding the impending "retirement" of The Honorable Robert E. Littlefield, Jr. on September 30, 2016, that Judge Littlefield will continue his judicial service in the Albany division of the Bankruptcy Court for the Northern District of New York on a recall basis. Judge Littlefield's recalled status has been approved by the Judicial Council of the Second Circuit, effective October 1, 2016. Judge Littlefield's recall assures our district that it will maintain three active judges pending the Judicial Conference of the 'United States' recommendations to Congress as to whether our temporary judgeship be made permanent, based, in part, upon case filing statistics.

Order Voiding Junior Mortgage Liens Pursuant to 11 U.S.C. 1322(b) and 506(a)

By: Cynthia Platt

The Board of Judges has approved a form order to be used for motions to void junior mortgage liens pursuant to 11 U.S.C. §§ 1322(b) and 506(a) granted in all divisions ("Pond Order"). The form Pond Order is posted to the court's website under Local Forms and is available by clicking here.

The form Pond Order provides for:

1. a junior mortgage and any claim filed by the junior mortgage holder to be treated as wholly unsecured during the pendency of a Chapter 13 case;

2. the junior mortgage to automatically become void, released and discharged upon the filing by the Chapter 13 trustee of a Certification of Completed Chapter 13 Plan with the court; and

3. the Debtor's presentment of a certified copy of the order and a copy of the Certification of Completed Chapter 13 Plan to the appropriate County Clerk who may mark the junior mortgage lien as discharged from the Debtor's residence.

Contact Us:

Albany:
US Bankruptcy Court
James T. Foley Courthouse
445 Broadway, Suite 330
Albany, NY 12207

Albany Clerk's Office Phone:
518-257-1661
Albany Help Desk:
518-257-1616

Syracuse:
US Bankruptcy Court
James Hanley Federal Bldg.
100 South Clinton Street
Syracuse, NY 13261

Syracuse Clerk's Office Phone
315-295-1600
Syracuse Help Desk:
315-295-1618

Utica:
US Bankruptcy Court
Alexander Pirnie Federal Bldg.
10 Broad St.
Utica, NY 13501

Utica Clerk's Office Phone:
315-793-8101
Utica Help Desk:
315-266-1118

Website Address:
http://www.nynb.uscourts.gov

District Case Assignments:

Case Series:	Direct Number
01-10	315-295-1653
11-19	315-295-1605
20-24	315-295-1606
25-28	315-295-1682
29-34	315-295-1686
35-43	518-257-1614
44-52	518-257-1607
53-62	518-257-1611
63-72	518-257-1633
73-82	315-266-1149
83-91	315-266-1108
92-00	315-266-1107

Credit Counseling

By: Kim Lefebvre

Effective February 15, 2016 Credit Counseling Certificates that are not timely filed or valid will be brought to the attention of the attorney for the debtor or the *pro se* debtor and if not cured within a reasonable time, an Order to Show Cause will be entered which directs the debtor and attorney to appear before the court and explain the failure. In addition, in the discretion of the court, dismissal of the case may result after the hearing.

The Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA) added an eligibility requirement for individual debtors. Unless granted a waiver of the requirement, "an individual debtor must now have received" … "during the 180-day period ending on the date of filing of the petition " … "an individual or group briefing" … "that outlined the opportunities for available credit counseling." **This is commonly referred to as the pre-filing credit counseling requirement.** This should not be confused with the post-filing requirement that individual debtors in chapters 7, 11 and 13 complete a course in personal financial management.

Debtors report whether they have satisfied the credit counseling requirement at *Part 5, Voluntary Petition for Individuals Filing for Bankruptcy* ("petition"). The Board of Judges has determined the clerk of court shall review this eligibility requirement and notify the assigned judge if the debtor has failed to timely attend credit counseling or failed to document their attendance by not timely filing the certificate issued by the provider.

Local Bankruptcy Rule Update

By: Diann Freeman

The Local Rules Standing Committee continues the important work of ensuring the court's local rules accurately reflect changes to the Code and Rules and local court practices. The Committee meets quarterly to consider the addition of new rules and modifications to existing rules. The public and members of the bar can submit a comment on the local rules at any time through the court's website at www.nynb.uscourts.gov. To date, in 2016, two local rules have been revised. Local Rule 4001-1 was revised on July 15, 2016. Local Rule 9013-3 was revised on July 18, 2016. Redlined and clean versions of the revised rules can be found on the court's website.

Attorney Practice Tips

By: Edward Didonna and Rochelle Murine

For any request to delay discharge or closing. Ask for an extension to a date certain, and calendar the date. The case may be discharged or closed without further notice.

Reaffirmation Agreements: File requests to delay chapter 7 discharge at least 48 hours prior to the discharge deadline. Chapter 7 cases are automatically discharged by the CM/ECF system the morning

Sites of Interest:

Pending Form Changes Effective December 01, 2016

http://www.uscourts.gov/rules-policies/pending-rules-amendments/pending-changes-bankruptcy-forms

Pending Rule Changes:

http://www.uscourts.gov/rules-policies/pending-rules-amendments

Federal Rules and Policies:

http://www.uscourts.gov/rules-policies

United States Trustee – Region 2:

https://www.justice.gov/ust-regions-r02

Electronic Bankruptcy Noticing:

http://ebn.uscourts.gov/

after the discharge objection deadline expires. Case administrators must mark the case docket in order to prevent cases from being discharged automatically by the system.

522(f) Motions and Other Post Discharge Activity: Cases may close automatically within two weeks of discharge. File motions as soon as practicable or, request a 30 day extension to delay closing and calendar the date. The case may close without further notice.

Motion to Reopen a Case for 522(f) Relief: Local Rule 5010-1(e) allows this motion to be brought on an Ex Parte basis. Review the rule for other ex parte motions.

The Loss Mitigation Procedures: Entering certain documents using the correct CM/ECF code alerts court staff to the filing of Loss Mitigation documents. If you are unsure of what CM/ECF entry to use, please contact the Court's Help Desk or the case administrator.

Save time and money: The court does not require chambers copies for claims, notices of appearance, amended schedules, orders, and any other non-motion related documents. Review Local Rule 9013-1(h) for required chambers copies. NOTE: The Clerk's Office may bill parties $0.50 per page to print copies for chambers.

Please link your documents: In CM/ECF, linking means relating your document to another document already filed in the case. For example, a notice of hearing is linked to the related motion; an objection or other responsive pleading is also linked to the related motion. As CM/ECF and our calendar program improve, more information can be gathered from the docket for use by all parties. Unlinked documents may hinder your ability to follow a motion or other action on a case docket and/or motion calendar.

Note on Using Fillable Forms: Generally, Official Forms are updated and released on December 1 with updates to the Federal Rules of Bankruptcy Procedure. However, local forms may be updated at any time to conform with local procedural changes and federal rules changes. Please review forms on our website for the most recent versions.

Chapter 13 Discharge- Shorten the Timeline: We notice the filing of the trustee final report and the default hearing for discharge within a few days of filing. We set a 30–day deadline for the Debtor's Certification Regarding Domestic Support Obligations and another 30 days for the hearing notice.

***You can file the Debtor's Certification as soon as the trustee files the final report. If we have the debtor education certificate and Debtor's Certification we will send the notice regarding the discharge hearing immediately.

Installment Payments: The clerk's office is now tracking installment payments by due date. If an installment payment is not paid by the date due, we mail a reminder notice to the debtor. When an installment payment is made, the due date deadline for that installment is terminated, and you are notified via Notice of Electronic Filing that a payment has been made.

PDF Size Increased: You may now upload documents as large as 35MB as one PDF. Tips for managing the size of PDFs:

- Documents created using word processing software are small files.

Pro Bono Attorney List:

Chief Judge Margaret Cangilos-Ruiz, Judge Robert E. Littlefield and Judge Diane Davis wish to acknowledge and thank the attorneys listed below for their public service to parties needing representation. During the last 12 months, these 54 attorneys assisted 165 debtors. Three attorneys served *pro bono* as a mediator.

Theodore L. Araujo
Michael D. Assaf
Michael J. Balanoff *
Paula M. Barbaruolo
Jerrold W. Bartman
Lawrence E. Becker
Neil T. Bhatt
Francis J. Brennan
Brian H. Bronsther
Michael A. Castle
Maxsen D. Champion
Robert H. Cohen
James S. Cox
Guy J. Criscione Jr
Richard Croak
James G. Cushman
Philip John Danaher
Nancy Baum Delain
M. Lettie Dickerson
Steven R. Dolson
Christian H. Dribusch
Marc S. Ehrlich *
Clifford C. Eisenhut
Susan N. Esce
Mary Lannon Fangio
Elizabeth Fletcher *
Robert H. Fix
Jeffrey Francisco
Gregory L Germai #
Kenneth W. Gibbons
Robert K. Greenough, Jr.
Kristie H. Hanson
Leigh A. Hoffman
William J. Leberman
Jason A. Little

- Documents uploaded as scanned images are larger files.
- Ensure that your scan settings are no higher than 300 DPI.
- To determine the size of a PDF, right click on the file and go to properties.

Using Internet Explorer 11 Instead of the Edge Browser in Windows 10

By: James Fleming

If you have upgraded your computer's operating system to Windows 10 or have purchased a new computer with Windows 10 preinstalled, please be aware that Microsoft's new Edge browser is the default web browser and can be accessed by clicking the  icon in the taskbar at the bottom of the Windows Desktop. The Edge browser is not presently supported by CM/ECF.

To resolve this problem, change your default browser to Internet Explorer 11 by completing the following steps:

1. Right-click the Windows icon -  - in the lower left corner of your Windows Desktop screen;
2. Click on Control Panel;
3. Click on Network and Internet;
4. In the left-hand column of options, click on Programs;
5. Under Default Programs, click "Set your default programs;"
6. In the list of programs, locate Internet Explorer and click on it, then click on "Set this program as default;"
7. Close Control Panel.

Internet Explorer 11 is now configured to be your default web browser.

You can 'pin' Internet Explorer 11 to the taskbar by following these steps:

1. Click on the Windows Explorer  icon in the taskbar.
2. Expand the C: drive, expand Program Files(x86), and expand Internet Explorer.
3. Right-click iexplore.exe and click on "Pin to taskbar."

You should now see the Internet Explorer  icon in the taskbar.

Finally, CM/ECF should be accessed in Internet Explorer in 'Compatibility View'. To access CM/ECF in 'Compatibility View',

1. Open Internet Explorer by clicking the Internet Explorer icon in the taskbar;
2. Browse to https://ecf.nynb.uscourts.gov;
3. Click on the gear icon  in the upper right hand corner of the browser;
4. Click on Compatibility View settings;
5. Verify uscourts.gov appears in the field below "Add this website", then click Add and Close.

You are now ready to use CM/ECF in Internet Explorer 11.

Pro Bono Attorney List Continued:

Merrit S. Locke
Carol Ann Malz
Zachary D. McDonald
Justin D Myers
Frederick W. Murad
Michael Jude O'Connor
Peter Alan Orville
Carol M. Dillon Pollard
David Allen Price
Michael Rhodes-Devey
Stephen T. Rodriguez
Richard J. Sardano
Randy J. Schaal
Peter C. Schaefer
David H. Swyer
Kevin B. Thiemann
Michael J. Toomey
Lee Matthew Van Houten
Meade H. Versace
Richard H. Weiskopf
L. David Zube

- Mediator Service

Syracuse University College of Law Bankruptcy Clinic

Flat Fee Increase in Albany and Utica

By: Elizabeth Vadney

Please be informed that Judge Littlefield has signed Administrative Order 16-03 and Judge Davis has signed Administrative Order 16-02 to increase the Chapter 13 Flat Fee by $125.00 to $4,325.00, effective April 1, 2016. The Orders are available on our website at www.nynb.uscourts.gov.

Changes to the Loss Mitigation Program Procedure and Forms

By: Elizabeth Vadney

The revised Loss Mitigation Program Procedures for the Northern District of New York Bankruptcy Court took effect **Tuesday, March 15, 2016**. In addition, the loss mitigation forms are either new or have been updated in connection with the revised Procedures. Beginning March 15, 2016, the new and revised forms should be used in all pending and new loss mitigation matters. The revised Loss Mitigation Program Procedures and the loss mitigation forms are available on the court's website: www.nynb.uscourts.gov.

Loss Mitigation Statistics for the Northern District of New York:

By: Elizabeth Vadney

The Loss Mitigation Program was initiated in the Northern District of New York on July 1, 2013. As noted in the procedure, "*The Loss Mitigation Program is designed to function as a forum in individual bankruptcy cases for debtors and lenders to reach consensual resolution whenever a debtor's principal residence is at risk of foreclosure.*"

Since the commencement of Loss Mitigation in our district, approximately 1453 Loss Mitigation Requests have been filed through July 1, 2016. We have lived with this new program for well over three years and have had an impressive number of requests. We enhanced our procedure effective March 15, 2016 through a committee consisting of bar members and court staff. Approximately 30 percent of chapter 13 filings include a loss mitigation request. That has remained constant since the commencement of the program.

Approximately 370 requests have been granted and 161 denied. However, many final reports have not yet been submitted due to trial modifications. Also, a denial is not specifically a failure. Pursuant to our final report, other outcomes, such as a short sale or surrender of property are a benefit to the debtor.

The procedures and forms for Loss Mitigation are available on our website at www.nynb.uscourts.gov.

Clerk's Office Awards Program:

Each year the Clerk's office holds a ceremony to honor employees who excel at their job and contribute significantly to the court's success or who share ideas that improve the court's methods, productivity and cost efficiency.

This year's award recipients are:

Darcy Davis – Utica
Colleen Johnson – Utica
Dorothy Glasheen – Syracuse
Lynn Chest – Albany
Frank Faragon – Albany
Cynthia Platt – Albany
Dawn Simmons – Syracuse
Jill Dalrymple – Utica
Robert Nussbaum – Syracuse
Tom Schaaf – Syracuse
Rochelle Murine – Syracuse
Dina McDonald - Albany

Awards are also given to employees for their years of dedicated government service. This years' service award recipients are:

Daniel Harrigan – 5 Years
Darcy Davis – 20 Years
Lisa Cardinal – 20 Years
Dina McDonald – 25 Years
Theresa O'Connell – 25 Years
Dina Ventura – 25 Years
Rochelle Murine – 25 Years
Kim Lefebvre – 35 Years

CM/ECF Training Classes – 3.5 Hours CLE Credit

By: Dina Ventura

Attorneys and staff may attend the class. Classes will be scheduled on an as needed basis in all three divisional offices. Interested parties may email CMECFTraining@nynb.uscourts.gov for additional information.

Notice Regarding Time Changes to the Albany Chapter 13 Calendar (Effective December 22, 2016)

By: Elizabeth Vadney

Effective December 22, 2016, the Albany Chapter 13 Calendar will have the following time changes:

- Chapter 13 motions shall still be heard at 9:15 a.m.
- Adjourned Chapter 13 motions shall still be heard at **10:00 a.m. instead of 12:30 p.m.**
- Chapter 13 Confirmations will now be heard at **11:00 a.m**. **instead of 12:15 p.m. and 12:30 p.m.**
- Chapter 13 claim motions and dismissal motions will now be heard **at 11:15 a.m.**

As December 22nd approaches will amend our Motion Dates Notice.

Notice Regarding Changes to Judge Davis' 2017 Motion Calendars

By: Colleen Johnson

Effective January 2017, the Utica Calendars will have the following changes:

- There will now be a stand alone Chapter 13 calendar and the Utica calendar will now include chapter 7, 12 and 13 Utica cases.
- Times have changed and all motion calendars have been made uniform
- Time for Loss Mitigation status hearings will now change to be heard along with companion matters.

How did you go bankrupt? Two ways. Gradually, then suddenly.

Ernest Hemingway

It always seems impossible until it's done.

Nelson Mandela

Bankruptcy is a serious decision that people have to make.

Herb Kohl

Coming together is a beginning; keeping together is progress; working together is success.

Henry Ford

No man is rich enough to buy back his past.

Oscar Wilde

Price is what you pay. Value is what you get.

Warren Buffett

Northern District of New York Bankruptcy Court Personnel Updates from Human Resources:

By: Sean Garrow

The past year brought some changes to the clerk's office and chambers' staffs in our bankruptcy court.

Clerk's Office

Annmarie Waters (IT Director) retired at the end of July, after more than 35 years of service. **Jim Fleming** (Systems Manager) has assumed responsibility for the management of the court's Information Technology department. **Lynn Chest** was appointed the CM/ECF Administrator. **Tony Lacey** (Programmer) transferred in July to the bankruptcy court for the Middle District of Alabama. The clerk's office is recruiting for a new Programmer.

Our court also welcomed some new employees. **Aaron Greth** (Financial Technician) began work in the clerk's office financial department in November 2015. **Sara Weiler** (Intake Clerk) accepted a position in July to work in the Syracuse Division of the clerk's office.

Chambers

Our judges' chambers experienced some transition as well.

Syracuse Chambers

Robert Nussbaum (Term Law Clerk to Chief Judge Cangilos-Ruiz) finished his two-year term and accepted an associate position at Milbank, Tweed, Hadley & McCloy, LLP in New York. **Michael Legge** (Term Law Clerk for Chief Judge Cangilos-Ruiz) began his term in September 2016. **Chase Bentley** (Cornell Law School)(Legal Intern) will begin working in Chief Judge Cangilos-Ruiz' chambers in January 2017.

Utica Chambers

Jaclyn Weissgerber (Term Law Clerk for Judge Diane Davis) finished her two-year term and is now term clerking for **Judge Walrath** of the Delaware bankruptcy court. **Lisa Taylor** (Term Law Clerk for Judge Davis) began her term in September 2016.

Albany Chambers

Ryan Hays (Term Law Clerk to Judge Littlefield) finished his two-year term and accepted an associate position at Cadwalder, Wickersham & Taft LLP in New York. **Matthew Zapala** (Term Law Clerk for Judge Littlefield) began his term in February 2016.

Uriel Pinelo (Albany Law School)(Legal Intern) began working in Judge Littlefield's chambers in August 2016.

Know what happens when an individual declares bankruptcy and how it affects his or her life.

Marilyn vos Savant

Do not dwell in the past, do not dream of the future, concentrate the mind on the present moment.

Budda

Some economists estimate that for every family that goes bankrupt, there are about 15 more who are in the same amount of financial trouble and would profit from bankruptcy but just haven't filed.

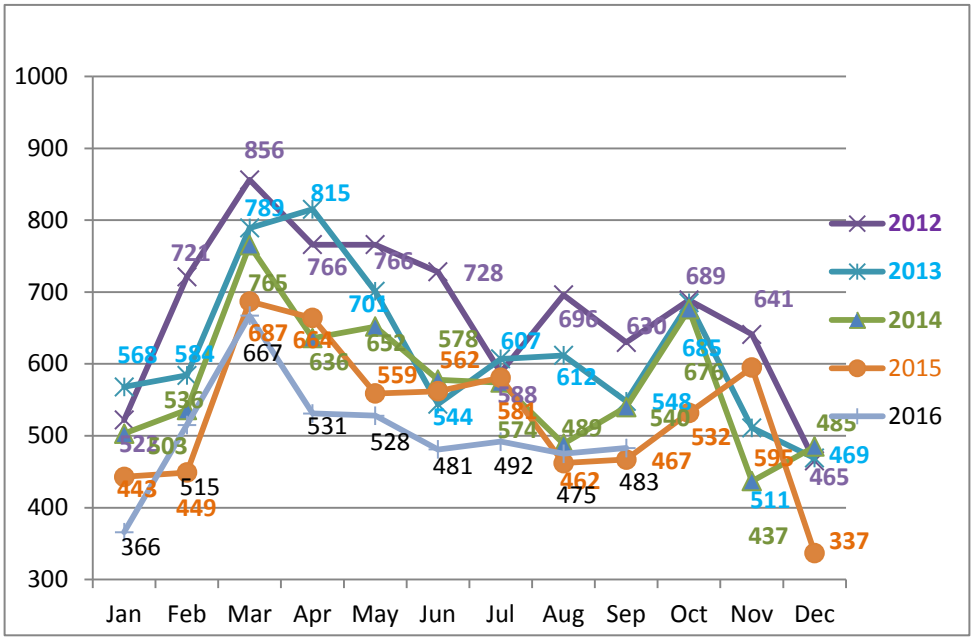
Elizabeth Warren

Yesterday is not ours to recover, but tomorrow is ours to win or lose.

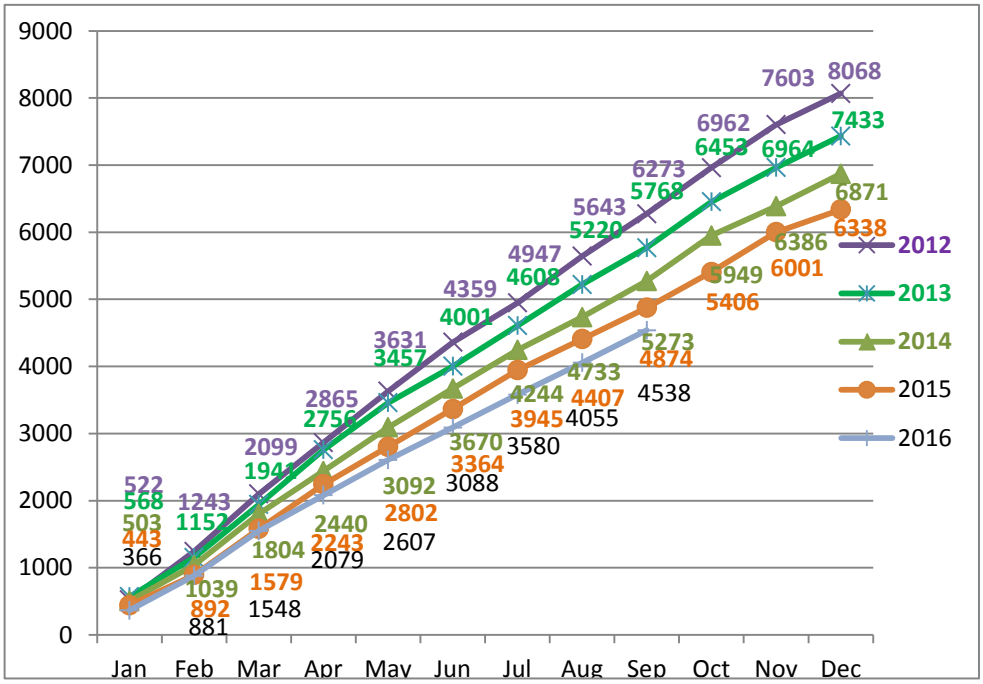
Lyndon B. Johnson

US Bankruptcy Court NDNY Case Filings Statistics

US Bankruptcy Court NDNY Case Filings by Month 2012-2016



US Bankruptcy Court NDNY Total Filings 2012-2016



ON THE RECORD WITH THE AO

By Scott Myers[1]

NEWS FROM THE ADVISORY COMMITTEE ON BANKRUPTCY RULES[2]

Bankruptcy Rules and Forms effective December 1, 2016

My fall column typically provides a brief preview of upcoming bankruptcy rule and form changes. This year there are 10 rule amendments, one new rule, and three official form amendments on track to go into effect on December 1, 2016:

The *Stern* Amendments (Rules 7008, 7012, 7016, 9027, and 9033).

Five of the amendments on track to go into effect this December -- to Bankruptcy Rules 7008, 7012, 7016, 9027, and 9033 -- respond to *Stern v. Marshall*, 131 S. Ct. 2594 (2011). Consistent with the United States Code, 28 U.S.C. § 157, the current Bankruptcy Rules distinguish between core and non-core bankruptcy proceedings and contemplate that a bankruptcy judge has more limited authority to resolve non-core proceedings. *Stern* held that a bankruptcy judge lacked authority under Article III of the Constitution to enter a final judgment in a proceeding that qualified as "core" under the Code, thus establishing that a proceeding could be "core" as a statutory matter but "non-core" (and thus non-permissible) as a constitutional matter. In response to *Stern*, the amendments propose three key changes: (1) they remove the distinction between "core" and "non-core" proceedings in the Bankruptcy Rules, namely in Rules 7008, 7012, 9027, and 9033; (2) they require parties to state at the outset whether they consent to entry of final orders or judgment by a bankruptcy judge in all adversary proceedings, not just in "non-core" proceedings as the current rules provide; and (3) they direct bankruptcy courts under Rule 7016 to decide the proper treatment of all proceedings, including whether to handle the proceeding at all, whether to entertain the proceeding and offer proposed findings of fact and conclusions of law, or whether to take some other action.

Elimination of the Three-Day Rule for Items Served Electronically

The Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure have long added three extra days to calculate time periods measured from certain types of service, most notably for service by U.S. mail. For some time, the three extra days have applied to filings served electronically. Each Advisory Committee affected by this convention agreed that the time for treating electronic service like mail service has passed and therefore recommended elimination of the three-day rule when a party receives service of an item electronically. The

---

[1] Scott Myers (Scott_Myers@ao.uscourts.gov) is an attorney in the Rules Committee Support Office of the Administrative Office of the United States Courts. His primary duties are to provide staff support for the Judicial Conference's Standing Rules Committee and its Advisory Committee on Bankruptcy Rules.

[2] This article will appear in an upcoming issue of the *American Bankruptcy Trustee Journal*. It is reprinted with the consent of the author and the *American Bankruptcy Trustee Journal*.

resulting package amends Bankruptcy Rule 9006(f) (as well as Appellate Rule 26(c), Civil Rule 6(d), and Criminal Rule 45(c)) to eliminate the three-day rule in cases of electronic service.

Procedures for International Bankruptcy Cases (Rules 1010, 1011, 1012, and 2002)

Three of the pending rule amendments, and the one new rule, facilitate the handling of international bankruptcy cases. The proposed new rule and amendments would: (1) remove the chapter 15-related provisions from Rules 1010 and 1011; (2) create a new Rule 1012 (Responsive Pleading in Cross-Border Cases) to govern responses to a chapter 15 petition; and (3) augment Rule 2002 to clarify the procedures for giving notice in cross-border proceedings.

Chapter 13 Notices (Rule 3002.1)

Bankruptcy Rule 3002.1 applies to chapter 13 cases and requires creditors whose claims are secured by a security interest in the debtor's principal residence to provide the debtor and the trustee notice of any changes in the periodic payment amount or the assessment of any fees or charges during the bankruptcy case. The rule is amended to clarify three matters over which courts have disagreed: (1) it applies whenever a debtor will make ongoing mortgage payments during the chapter 13 case, regardless of whether a prepetition default is being cured; (2) it applies regardless of whether it is the debtor or the trustee who makes the mortgage payments; and (3) it generally ceases to apply when an order granting relief from the stay becomes effective with respect to the debtor's residence.

Official Forms 420A, and 420B.[3]

Official Forms 420A, (Notice of Motion or Objection), and 420B, (Notice of Objection to Claim), are renumbered (from 20A and 20B) to comport with the form numbering style developed as part of the Forms Modernization Project. The forms are also amended to change the phrase "mail" to "send" to reflect the fact that there are various methods of providing documents to other parties.

Official Form 410S2

Official Form 410S2, (Notice of Postpetition Mortgage Fees, Expenses, and Charges), is amended in the instructions in Part 1 to clarify how to report previously approved fees, expenses, or charges. The following language is added: "If the court has previously approved an amount, indicate that approval in parentheses after the date the amount was incurred." This amended language replaces the prior instruction not to report any amounts previously ruled on by the bankruptcy court.

Rules and Forms Published for Comment

[3] Copies of the proposed forms are on the "pending forms page" of judiciary's public website: http://www.uscourts.gov/rules-policies/pending-rules-amendments/pending-changes-bankruptcy-forms

Bankruptcy rule and forms amendments are generally published for public comment for approximately six months from mid-August to mid-February. This year, however, there were two separate publications. The first publication began on July 1, 2016 and the second began on August 15, 2016.

July 1, 2016 Publication—Bankruptcy Rules 3015 and 3015.1 and Chapter 13 Plan Form Package

In 2011, the Advisory Committee on Bankruptcy Rules began considering creation of an official form plan to be used in chapter 13 cases. The proposed form and proposed amendments to nine related rules were published for comment in August 2013 and again in August 2014.

At its fall 2015 meeting, the Advisory Committee approved the plan form (Official Form 113), and amendments to eight of the related rules—Bankruptcy Rules 2002, 3002, 3007, 3012, 4003, 5009 7001, and 9009—but voted to defer submitting those items to the Standing Committee.[4] As a result of the comments received during the 2014 publication, the Advisory Committee proposed and the Standing Committee agreed to republish for comment one of the initial nine rules, (Rule 3015), and new Rule 3015.1. Rules 3015 and 3015.1 introduce for the first time the possibility of a district-by-district opt-out from the national form plan concept, as long as the opt-out district adopts a local district-wide form plan that meets the requirements set forth in the new rule.

Rules 3015 and 3015.1 were published for comment for a three-month period—July 1, through October 3, 2016. The Advisory Committee published the rules for a shortened time frame in order to receive comments from the public while still leaving open the possibility of seeking approval of the chapter 13 plan form and the related rules in time for the full package to go into effect by December 1, 2017.

August 15, 2016 Publication

The August 2016 request for public comments consists of proposed changes to:

- Rule 3002.1(b) (Notice of Payment Changes) and (e) (Determination of Fees, Expenses, or Charges),
- Rule 5005(a)(2) (Electronic Filing and Signing),
- Rule 8002(b) (timeliness of tolling motions),
- Rules 8013, 8015, 8016, 8022, Official Form 417C, and Part VIII Appendix (length limits),

[4] The latest available versions of the proposed amendments to Rules 2002, 3002, 3007, 3012, 4003, 5009 7001, and 9009 are included in the Addendum (a related download) to Bankruptcy Rules Committee's October 2015 agenda materials beginning at Tab 4, page 53. http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-bankruptcy-procedure-october-2015.

- Rule 8017 (amicus filings),
- Rule 8002(a) (separate document requirement),
- Rule 8006(c) (court statement on merits of certification),
- New Rule 8018.1 (district court review of a judgment that the bankruptcy court lacked constitutional authority to enter),
- Rule 8023 (voluntary dismissal; cross-reference regarding settlements), and
- Official Form 309F (Notice of Chapter 11 Bankruptcy Case (For Corporations and Partnerships)).

Although the public comment period for the July Publication will likely be closed by the time this article is published, readers are encouraged to review the proposed amendments and new rules and forms that make up the August Publication and to submit comments. Copies of the proposed amendments for both publications should be available on the judiciary's public website at the following link: http://www.uscourts.gov/RulesAndPolicies/rules/proposed-amendments.aspx

Comments can be submitted by email at rules_comments@ao.uscourts.gov. The deadline for submitting comments addressing the amendments in the August Publication is February 15, 2017.

Reprinted with permission from: New York State Bar Association *Journal*, May 2016, Vol. 88, No. 4, published by the New York State Bar Association, One Elk Street, Albany, NY 12207

Dino E. Medina serves as general counsel at Complete Discovery Source, Inc. (CDS), a leading provider of electronic discovery services and a leading developer of data management solutions. In this capacity, Mr. Medina advises CDS on a variety of legal matters, including employment issues, contract drafting and negotiation strategies, dispute resolution, data privacy, security and compliance. Mr. Medina is a member of the New York Bar and the Electronic Discovery Committee of the New York State Bar Association. He teaches and speaks frequently on eDiscovery hot topics and best practices for deployment of legal technology. Mr. Medina lives on Long Island, New York with his wife and two children. This article is for informational purposes only and is not intended to constitute legal advice or to be relied upon.

Defensible Cybersecurity

Tailoring an Organization's Security Posture to Applicable Legal Standards

By Dino E. Medina

It's not surprising that security experts now regularly use phrases like "There are companies that have been hacked, companies that don't know they've been hacked, and companies that refuse to recognize they have been hacked." Although the storage of sensitive information in the digital space is the modern, convenient, cost-effective norm for law firms and the corporate entities they serve, the potential for misappropriation of this information is greater than ever. Over the past couple of years, data breaches stemming from both hackers and inadvertent disclosures have increased exponentially.

Everyone is talking about security, but how does such talk translate to a provable, defensible cybersecurity program? Law firm clients, corporate investors and regulators (collectively, stakeholders), now closely scrutinize the security measures of law firms and corporate entities, respectively, with the goal of creating greater accountability for the security of their sensitive electronic data. These organizations have responded by hiring outside consulting firms to build custom information security management systems.

What looks solid on the surface may sit on unstable ground. The creation of a typical information security management system entails conducting a risk assessment, creating security policies and testing the effectiveness of those policies. While a well-designed information security management system can provide a superficial level of assurance to stakeholders, the failure to place applicable legal standards for data security at the forefront of each stage of the program-building process is likely to result in

the subject entity's inability to mitigate damages should an actual data breach occur.

John Verry, managing partner at Pivot Point Security, explains,

> It's hard to over-emphasize the value of strong risk assessment capabilities when building a comprehensive and provable information security program. It is only through the broader consideration of "non-traditional" information-related risks such as physical security, employees, contractual risk, laws/regulations, vendors and partners that an organization can protect itself from the diverse threats that are often the cause of today's largest breaches.

To better explore this issue, we set forth the elements used to assess an entity's security posture prior to the policy planning stage, offer a set of best practices to guide policy development, identify the types of accreditations available to such entities and illustrate how incorporation of applicable legal standards into each of these processes results in the most effective security risk mitigation system.

Key Risk Assessment Considerations

There are a number of formal data security risk assessment methodologies in existence, each with a different name applied to legitimize its application to a particular data type, industry, or set of activities. However, there are two elements that tie them all together – their purpose is to understand what risks exist to the entity applying them, and to document the likelihood and impact of each known risk.[1] The central question in any data security risk assessment is: Are the precautions an entity takes to secure its electronic data effective at controlling the types of risks the entity faces?

Identify Sensitive Data and Categorize It According to Applicable Legal Standard

The first step in the assessment process is to evaluate the sensitive data types the subject entity creates, collects, maintains or transmits, and categorize this data based on the legal framework governing its protection. Law firms and their corporate clients hold a variety of sensitive data types, each requiring a different standard for protection. Here are some examples of sensitive data types and the legal standard(s) applicable to the security of each.

The security of information an attorney learns during the representation of a client, including a corporate client, is governed by ethical standards for attorney conduct. For example, the American Bar Association's Model Rule 1.6(c) states "a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to the representation of a client."[2] The comments to Rule 1.6 set forth factors that are to be used to determine the reasonableness of an attorney's efforts to secure his or her client's information. They include the below items.[3]

- Sensitivity of the information
- The likelihood of disclosure if additional safeguards are not employed
- The cost of employing additional safeguards
- The difficulty of implementing the safeguards
- The extent to which the safeguards negatively impact the lawyer's ability to represent clients generally

Personally Identifiable Information (PII) is any information about an individual maintained by an entity, including (1) any information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security number, date of birth); and (2) any other information that is linked or linkable to an individual (e.g., medical, financial and employment information). Forty-seven states have implemented such laws and each requires appropriate administrative, technical and physical safeguards for PII.

Protected Health Information (PHI) is information traceable to a patient by one or more of 18 identifiers that relate to medical condition, diagnosis or treatment,[4] including:

- Name
- License number
- Dates (e.g., birth, admission, discharge, death)
- Vehicle identifiers
- Address
- Medical device identifiers
- Phone number
- Fax number
- URLs
- IP address
- Email address
- Biometric identifiers
- Facial photographs
- Social Security number
- Health plan number
- Medical record number
- Account number
- Any other unique identifier

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI. The standard for satisfaction of the Security Rule is encryption of electronic PHI.

The security of intellectual property (IP) is typically governed by contract, applying a standard of care that the party receiving IP information uses to protect its own information of like importance. IP, whether in the form of patents, trademarks, copyrights or trade secrets, may be more valuable than an entity's physical assets. According to the Commission on the Theft of American Intellectual Property, U.S. companies lose hundreds of billions of dollars each year as a result of IP theft.[5]

Once sensitive data and the legal standards applicable to their security are identified, it is time to understand and analyze the entity's security risks. For this step, it is necessary to examine all forms of risk that potentially impact security of sensitive data, including without limitation, regulatory risk, technical risk (i.e., gaps in the entity's physical and virtual security infrastructure), risk of human error (e.g., susceptibility to phishing, ransomware or malware attacks), risks in physical security infrastructure (i.e., all points of entry into areas where sensitive data resides, including buildings, offices and server rooms), and risks in virtual security infrastructure (e.g., network access controls, software access controls, password protocols, and encryption of data in motion and data at rest[6]).

Assemble the Team

The next step in the assessment is to evaluate the entity's internal resources and assemble a team with the types of expertise necessary to thoroughly address the organization's risk posture. There are four categories of personnel required for this step:

- Legal personnel to advise with respect to the laws applicable to the data the entity holds;
- Technical personnel to advise with respect to software and infrastructure;
- Accounting personnel to advise with respect to the costs versus benefits of existing cyber-risk controls; and
- C-suite personnel for analysis of business processes applicable to sensitive data, whether there's existing organizational buy-in of risk mitigation strategies, and whether existing security controls are inhibiting the entity's growth progress.

The final component of the security assessment stage is to bring the entity's key teams together to link the business processes that access sensitive data, the people and technology used to support those processes, and the existing security structure to evaluate areas of risk. This task requires the drafting of a risk assessment report in order to comprehensively address data security risks. Law firms and corporate entities should consider engaging an outside expert to assist in this task, as holes in risk assessment documentation will result in an ineffective cybersecurity program.

Drafting Effective Information Security Risk Management Policies

Once the law firm or corporate entity has assessed its data security risks using this framework, it needs to carefully craft information security management policies to control these risks.[7] To meaningfully address an organization's risk profile, the risk assessment report and legal standards governing security of the data must guide policy development. When drafting the policies, remember to include the following, often-overlooked, aspects:

- Closely link the legal standards governing security of the sensitive data to the policy requirements;
- Include verification of the entity's continuing compliance with the policies;
- Incorporate comprehensive employee training with periodic updates into the program, since studies have found that educating employees is vital to reducing data breaches;[8]
- Ensure third-party security risks are effectively managed;
  - Via contract, make certain they are legally bound to maintain data security in accordance with stan dards applicable to your sensitive data types, and
  - Stipulate audit requirements, recognizing the third-party vendors' confidentiality obligations to other clients.

Third-Party Verifications

If an entity's underlying information security methodology is properly designed and effectively implemented, external security verifications can both instill confidence in stakeholders and substantially mitigate damages in the event of a security breach. They can be used to test a law firm or corporate entity's own data security controls and those of its outside contractors. Various levels of external testing, audits and security accreditations are available, including the following – listed in order of testing rigor:

- SSAE-16 SOC 1 (Standard for security controls impacting financial reporting)
- SOC 2 (Standard for security, availability, processing integrity, confidentiality or privacy of information)
- ISO-27001: 2013 (International standard for information security)
- PCI DSS (Payment Card Industry standard for merchants)
- FedRAMP (U.S. Government standard for cloud services providers)

SSAE-16 SOC1 Type 2 Standard

The Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) published the Statement on Standards for Attestation Engagements (SSAE) No. 16 – Reporting on Controls at a Service Organization – in January 2010. The ASB defines a service organization as one that provides services to "user entities," for which these services are likely to be relevant to the user entities' own internal controls for financial reporting.[9] The term "user entity" is simply an entity utilizing the services of a service organization.

The SSAE 16 standard requires a service organization to describe its "system" (i.e., the services the organization provides, along with the supporting processes, policies, procedures, personnel and operational undertakings that constitute the service organization's core activities relevant to user entities). In addition, management of the service organization must make a number of affirmative,

written representations regarding its systems and the appropriateness of the design and operating efficacy of the organization's controls in satisfying their objectives[10] – for purposes of this article, the objective is information security, and the areas requiring management representations follow.

- Management's description of the service organization's "system" has to fairly and accurately represent the "system" as implemented throughout the time period subject to testing, which is typically six months.
- The control objectives referenced in management's description of the service organization's "system" have to have been appropriately designed to achieve those control objectives throughout the time period subject to testing; again, to be effective, the control objectives must closely track applicable legal standards.
- The controls have to have been consistently applied throughout the time period subject to testing.

An SSAE 16 information security audit and resulting report would include testing of the integrity, security and privacy of client data. Entities providing material outsourcing services to other entities (e.g., a law firm hosting client data for litigation purposes) would be well-advised to consider SSAE 16 third-party compliance examinations as a means of providing ongoing data privacy assurances to stakeholders and mitigating damages when a data breach occurs.

SOC 2 Standard

The AICPA Assurance Services Executive Committee released the current version of the Service Organization Control (SOC) 2 framework in January 2014. SOC 2 is a criteria-based framework that reports on a service organization's controls over one or more of the below Trust Services Principles (TSPs).[11]

- Security of a service organization's system (see SSAE 16 for "system" definition)
- Availability of a service organization's system
- Processing integrity of a service organization's system
- Confidentiality of the information that the service organization's system processes or maintains for user entities
- Privacy of personal information that the service organization collects, uses, retains, discloses and disposes of for user entities

An entity employing the SOC 2 framework may omit one or more of the five TSPs from the scope of its audit, provided each of the omitted TSPs is not applicable to the system under audit.[12]

Similar to an SSAE 16 information security audit, a SOC 2 audit would include testing of the subject entity's integrity, security and privacy of client data; however, there are two key differences: (1) as noted above, the SOC 2 TSPs include testing of additional system availability and information privacy controls; and (2) SOC 2 is tailored to technology and cloud computing service organizations, incorporating the TSPs in accordance with the Attestation Standards (AT) Section 101. Law firms and corporate entities storing client data in electronic form should consider SOC 2–based third-party compliance examinations as an alternative to SSAE 16 to bolster security and soften exposure should a data breach occur.

ISO-27001: 2013 Standard

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Joint Technical Committee published the ISO/IEC 27001:2013 information security standard in October 2013. It is a benchmarks-driven, internationally accepted specification for establishing, implementing, maintaining and continually improving an entity's information security management system (ISMS), covering both the entity's internal sensitive information as well as sensitive information entrusted to the entity by third parties.[13] The ISO/IEC 27001:2013 standard includes requirements for the assessment and treatment of an entity's information security risks that are custom-designed to address the entity's specific information security risk profile. Organizations meeting this security standard may gain an official certification issued by an independent and accredited certification body upon successful completion of a formal audit process.

> Once sensitive data and the legal standards applicable to their security are identified, it is time to understand and analyze the entity's security risks.

ISO certifications are effective for three-year periods, provided the entity successfully completes interim annual spot inspections which demonstrate its ongoing compliance with the customized ISMS. More than the SSAE and SOC 2 attestations, the ISO/IEC 27001:2013 standard and its related benchmarks can act as guidelines for entities wishing to design defen-

sible data security protocols. The benchmarks cover 14 domains:

- Information security policies tailored to legal/regulatory requirements
- Organization of information security
- Human Resources security (pre-employment, during employment and post-employment)
- Asset management
- Access control
- Cryptography
- Physical security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity
- Compliance with ISMS policies and applicable laws

PCI Standard

The Payment Card Industry (PCI) Security Standards Council launched the PCI Data Security Standard (DSS) in December 2004. The PCI DSS applies to any merchant, including any law firm or other corporate entity, which processes, stores or transmits credit card information. It requires a robust set of administrative, technical and physical security controls, including:[14]

- Install and maintain a firewall configuration to protect cardholder data
- Prohibit the use of vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Protect all systems against malware, and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique user ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for all personnel

It is important to note that although all merchants that process, store or transmit cardholder data must implement and adhere to the PCI DSS, formal certification of PCI DSS compliance is not required for all merchants, particularly smaller ones. Nonetheless, to avoid liability for fraud associated with theft of cardholder data, law firms and other entities subject to PCI DSS are wise to undergo formal audits.

FedRAMP

Finally, the most comprehensive data security attestation is the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP was implemented in December 2011 to provide assurances regarding the security of government data stored in cloud environments. It is a government-wide, standardized approach to security assessment, authorization and continuous monitoring for cloud-based products and services.[15] FedRAMP certification is a requirement for law firms and corporate entities seeking to host government data in a cloud-based (i.e., Internet-accessible) format.

The FedRAMP process incorporates the following five-step approach to certify a cloud-based service provider's (CSP) authorization to host government data:

1. Authorization Initiation: Federal agencies or CSPs initiate the FedRAMP process by pursuing a security authorization. There are two sub-steps to complete here.
   - Submit a formalized request for Authority to Operate (ATO) as a government CSP to the FedRAMP Joint Authorization Board (JAB);
   - Document and implement the required security controls and policies based on the level of risk posed by the types of government data at issue and the type of cloud system in which the CSP will store that data. Entities with other security accreditations (e.g., ISO/IEC 27001:2013) can leverage existing policies for this sub-step to save time, money and resources.
2. Security Assessment: The security assessment process must be conducted by an accredited third-party assessment organization (3PAO) and incorporates a set of baseline security controls for information technology systems developed by the National Institute of Standards and Testing (i.e., NIST SP 800-53 Rev. 3).
3. Review: 3PAOs send security assessment packages to the FedRAMP JAB for review.
4. Authorization: CSPs continue to work with federal executive departments and agencies to obtain ATO permissions.
5. Ongoing Compliance: Once an ATO is granted, ongoing security assessment and authorization activities must be satisfied to maintain the ATO.

The common link to all cyber security programs is their focus on the subject entity's operational controls within a risk framework that is acceptable to that entity.[16] The primary factors that influence an entity's acceptable levels of risk include:

- Legal requirements
- Client-specific requirements
- Amount of physical and monetary resources available for data security
- Types of data held
- Business sector in which the entity operates

Law firms and the corporate entities they serve act as vast repositories of both commercially sensitive information and

PII, including PHI. The unauthorized disclosure of this kind of information could have a devastating effect on the responsible entity's reputation, financial position and, ultimately, the entity's ability to remain in business. Given the potential losses at stake when a data breach occurs, law firms and corporate entities must develop comprehensive cybersecurity programs, placing chief importance on the legal standards relevant to protecting their sensitive information.

1. https://www.optiv.com/blog/conducting-a-risk-assessment-key-components-you-cant-ignore.

2. http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.

3. *Id*.

4. *See* 45 C.F.R. § 164.103.

5. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf, p. 1.

6. Data in motion is data that is exiting an entity's network via email, the web or other Internet protocols, while data at rest is data in computer storage (e.g., data on a file server, hard drive or backup tape).

7. In addition to written policies, implementation of technical controls/standards/procedures (e.g., a state-of-the-art firewall, ant-virus software) is essential to a comprehensive cyber risk management program.

8. http://www.cio.com/article/2384855/compliance/most-data-breaches-caused-by-human-error--system-glitches.

9. http://www.ssae16.org/important-elements-ssae16/what-is-a-service-organization.

10. *Id*.

11. http://www.ssae16.org/white-papers/soc-2-reporting-framework-essentials-part-i.

12. *Id*.

13. http://www.iso.org/iso/catalogue_detail?csnumber=54534.

14. http://searchsecurity.techtarget.com/definition/PCI-DSS-12-requirements. Though framed as a legal standard herein, the PCI DSS is used by financial institutions as a formal risk assessment and compliance tool for merchants.

15. https://www.fedramp.gov/about-us/about/.

16. In the case of a FedRAMP-based cybersecurity program, acceptable risk levels are ultimately determined by the government agency engaging the CSP.