Clerk's News

October 09, 2015 **Volume 1, Number 1** **Editors: Diann Freeman and Dina Ventura**

In This Issue:

Two Bankruptcy Software Vendors to Cease Product Support

By: AnnMarie Waters and Diann Freeman

EZ-FILING DISCONTINUING SUPPORT AND UPDATES

The Bankruptcy Court for the Northern District of New York has been notified that EZ-Filing is discontinuing support and updates to its bankruptcy petition preparation software. Please be advised that CINgroup, the parent company of Best Case Bankruptcy, EZ-Filing, CINcompass, CIN Legal Data Services and Suite Solutions, will no longer update or support EZ-Filing software after November 30, 2015 due to the extensive proposed bankruptcy form changes. If you are currently using EZ-Filing software, you may have already received notification directly from CINgroup regarding this announcement.

NEW HOPE SOFTWARE, INC. DISCONTINUED

CINgroup has acquired the assets of New Hope Software, Inc. Due to the significant changes required for the December 2015 forms update, New Hope Software, Inc. has elected to discontinue development and sales of its Bankruptcy 2015™ filing software. Former or prospective customers should contact CINgroup regarding update options.

Federal Bankruptcy Forms Update Effective December 01, 2015

By: AnnMarie Waters and Dina Ventura

As part of the forms modernization project most official bankruptcy forms will be replaced with substantially revised, reformatted and renumbered versions effective December 01, 2015. The new forms are available on the US Courts website: http://www.uscourts.gov/rules-policies/pending-rules-amendments/pending-changes-bankruptcy-forms

The CM/ECF Case Opening screens will be modified to include additional information effective December 01, 2015. These changes can be viewed in our CM/ECF test database https://ecf-test.nynb.uscourts.gov/

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

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

Syracuse Clerk's Office Phone
315-295-1600

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

Utica Clerk's Office Phone:
315-793-8101

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

District Case Assignments:

Case Series:	Direct Number:
01-09	315-295 -1653
10-18	315-295 -1605
19-27	315-295 -1606
28-29	315-295 -1682
30-35	315-295 -1686
36-44	518-257 -1614
45-53	518-257 -1607
54-62	518-257 -1611
63-71	518-257 -1633
72-81	315-266 -1149
82-90	315-266 -1108
91-100	315-266 -1107

Bankruptcy Rule Amendments – Effective December 01, 2015

By: Kim Lefebvre

Bankruptcy Rule changes are limited to the amendment of one rule –

Rule 1007. Lists, Schedules, Statements, and Other Documents; Time Limits.

Subdivisions (a)(1) and (a)(2) of Rule 1007 require the filing at the outset of a case of the names and addresses of all entities included on "Schedules D, E, F, G, and H." The restyled schedules for individual cases to be effective December 1, 2015 use slightly different designations. Under the new numbering and lettering protocol of the proposed forms, the schedules referred to in Rule 1007(a)(1) and (a)(2) will become Official Forms 106 D, E/F, G, and H — reflecting a combination of what had been separate Schedules E and F into a single Schedule E/F. In order to make Rule 1007(a) consistent with the new form designations, the amendments change references to Schedules E and F to Schedule E/F.

GovDelivery is here!

By: AnnMarie Waters

We are pleased to offer a free email subscription service allowing you to receive periodic notification updates from the court. This service allows subscribers to receive notifications by email when new information is available such as local rule changes, calendar updates, and other alerts. You will only receive email updates on topics that you specify. You may unsubscribe at any time.

Please visit our website www.nynb.uscourts and click on the link  to sign up.

CM/ECF Training Classes – 3.5 CLE Credits

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.

Update Regarding CourtSpeak and the Audio Record of Court Hearings

By: Elizabeth Vadney

The CourtSpeak pilot program has been in place since March 2015 in our Syracuse division. It has proven to be a useful resource for both

Sites of Interest:

Pending Form Changes Effective December 01, 2015
http://www.uscourts.gov/rules-policies/pending-rules-amendments/pending-changes-bankruptcy-forms

Pending Rule Changes Effective December 01, 2015
http://www.uscourts.gov/rules-policies/pending-rules-amendments/pending-changes-bankruptcy-forms

Federal Rules & Policies:
http://www.uscourt.gov/rules-poilices

United States Trustee – Region 2:
http://www.justice.gov/ust-regions-r02

Electronic Bankruptcy Noticing:

http://www.ebnuscourts.com/

Bankruptcy Recourses and Reference Materials

https://www.law.cornell.edu/wex/bankruptcy

the court and attorneys. Its benefits include:

- Ready access to case information;
- The ability to review exactly what the court stated at a hearing, thus increasing the accuracy of proposed orders and compliance with directives;
- Ease of review of a proceeding that an attorney is interested in following, but not directly involved with; and
- Cost savings. Attorneys no longer need to purchase an audio CD for $30 to listen to a hearing. PACER users have one-time free access to an audio file. Subsequent access is billed at only $2.40 per audio file.

The court is interested in your opinion on the usefulness of this new technology. Please share with a member of the court staff your experience with CourtSpeak. The other divisions may also begin using CourtSpeak in the future. You will be notified in advance if this occurs.

Intra-District Transfers – Venue Conflicts

By: Edward Didonna

The Clerk's Office relies on Post Office mailing data to determine the county of residence whenever there is a venue conflict. Please refer to Local Bankruptcy Rule 1073-1 for guidance.

In rare instances, there will be conflicting venue information. To ensure that a case is not erroneously re-assigned, file a statement concerning venue and attach a copy of the property tax bill. Venue will be determined by the county to which the debtor pays property taxes.

Intra-District Transfers – Issues Concerning Case Transfers between Divisional Office's with the Opening of the Syracuse Clerk's Office and Chambers

By: Edward Didonna

In 2007 and 2008, the counties were apportioned among three district offices. This re-apportionment included the transfer of active cases to the new divisional office and re-assignment to that particular judge. The transfer of cases between districts also meant a change in the case numbers for the affected debtors.

One consequence of the change in the case numbers is that the debtor's credit report may show two bankruptcy cases filed, rather than one. In those instances where the duplication is the result of a case transfer, and not multiple filings, the Clerk's Office can assist the

Pro Bono Attorney List:

Chief Judge Cangilos-Ruiz, Judge Littlefield and Judge Davis commend attorneys who have selflessly given of their time and resources to assist petitioners and litigants in our bankruptcy court. Their pro bono representation reflects compassion for the parties and desire to do the public good.

Attorneys with five or fewer Pro Bono Cases:

Arthur D. Agnellino
Michele L. Anderson
Lawrence Becker
William F. Berglund
Darrell L. Bowen
Francis J. Brennan
Maxsen D. Champion
Robert H. Cohen
James S. Cox
James G. Cushman
M. Lettie Dickerson
Russell W Dombrow
Edward D. Earl
Peter G. Ford
Eric R. Gee
Richard W. Gunger
Kristi H. Hanson
Carl W. Hasselbarth
Opal Fayne Hinds
Peter M. Hobaica
Anthony Inserra
Robert L. Katzman
Merritt S. Locke
Justin M. Nackley
Carol Dillon Pollard
Martin W. Pozefsky
Rachel A. Rappazzo
Paul B Sherr
Peter N. Talev
Richard H. Weiskopf
Stewart L. Weisman
L. David Zube
David C. Alexander
Brian H. Bronsther
Guy J. Criscione Jr.
Heidi Dennis
David F. DeVall
Cindy Domingue-Hendrickson
Jeffrey L. Drimer

debtor with an explanation and supporting documentation for the credit reporting agencies.

Upon request, we will provide the debtor with the following information at no charge:

- A customized cover letter with an explanation of the change in counties and resulting case number change;
- A certified copy of the order transferring the case within district;
- A certified copy of both dockets.

Please have debtors contact an Operations Supervisor for assistance with this matter: 315-295-1636 or 518-257-1632.

Updated Pro Bono and Pro Se Information on Court's Website

By: Edward Didonna

We have improved and expanded the resources available to parties considering Pro Bono or Pro Se representation.

Under the "Finding Legal Assistance" tab, we have links to legal and housing services, as well as links to other consumer information resources. Please take a look at these links, since some of them may be unfamiliar to you.

Under "Filing Without an Attorney" we have links to the US Court's web page as well as the Code and Rules, and the US Trustee website. There is also a copy of the "Pro Se Packet" with active links to forms, specific code and rule cites, and helpful information.

Pro Se cases are labor intensive and have the potential to strain limited resources in the Clerk's Office. We actively encourage the public to seek professional legal advice to assist with the process. There are warnings and suggestions throughout the web pages and in the documents.

Please review our website. We would appreciate your comments and suggestions to improve upon the information provided. If you believe there are documents, checklists, or FAQs that would be helpful, please let us know. It is important to have informed consumers.

Pro Bono Attorney List Continued:

Attorneys with five or fewer Pro Bono Cases:

Carol Ann Malz
Zachary DeCurtis McDonald
Peter A. Orville
Michael Rhodes-Devey
Meade H. Versace
Michael D. Assaf
Donald W. Biggs
Richard Croak
Nancy Baum Delain
Thomas P. Hughes
Justin D Myers
David Allen Price
Stephen T . Rodriguez
Mary Lannon Fangio
Jerrold W. Bartman
Samuel B. Warner

Attorneys with six to ten Pro Bono Cases:
Christian H. Dribusch
Susan N. Esce
Gregory L Germain*
Jonathan D. Warner
Alan R. LeCours Sr.
Paula M. Barbaruolo
* Syracuse Law School Legal Clinic

Attorneys with eleven to fifteen cases Pro Bono Cases:
Marc S. Ehrlich
Michael J. Toomey

Attorneys with more than fifteen Pro Bono Cases:

Lindy M Madill
R. Thomas Miller
Michael J O'Connor

Ira Lobel**

** Mediation Services

Requesting Discharge on Behalf of Deceased Debtors

By: Edward Didonna

Waiver of Requirement to Complete and File a Personal Financial Management Certificate, *Post-Petition* for Individual debtors under Chapter 7, 11, and 13:

Local Rule 1007(f)(2): **Deceased Debtor Excused from Compliance**. If a debtor dies after the filing of the petition and prior to completing the course in financial management, the debtor's attorney may file an ex parte application requesting a waiver of the completion of the course. A redacted version of the death certificate shall be attached as an exhibit to the application with service on the US Trustee and the case trustee.

Waiver of Requirement to File Certification Regarding Domestic Support Obligations, 11 USC §522(q) and §1228 (ch 12) or §1328 (ch 13):

Local Rule 4004-1(b)(2): **Request for Waiver of Certifications for Deceased Debtor.** Upon ex parte application and submission of a proposed order, the court may consider the waiver of certifications required under LBR 4004-1(b) for a deceased debtor. The ex parte application must be supported by a properly redacted death certificate

New CM/ECF category has been created

By: Edward Didonna and Dina Ventura

A new category has been created in CM/ECF under the "Adversary" menu entitled "Adversary Miscellaneous."

All the CM/ECF events filed that apply to adversary complaints have been reproduced under this newly created "Adversary Miscellaneous" category. You may, however, still find the events listed under the Bankruptcy category.

You may need to clear your internet browser's "cache" to see the newly created category in CM/ECF. Instructions for clearing cache may be found on our Court's website under CM/ECF > CM/ECF Miscellaneous News and Instruction.

Reminder concerning Local Rule 7003-1 – Adversary Proceeding Cover Sheet

By: Edward Didonna and Dina Ventura

All adversary complaints, including complaints filed via the CM/ECF system, must have an Adversary Proceeding Cover Sheet, Official From 104, attached. The Clerk's Office relies on the coversheet for

Local Rule Standing Committee List:

Paula Barbaruolo
518-782-9100
pbarbaruolo@pmblawpc.com

Michael J. Balanoff
315-703-6545
mbalanoff@lscny.org

Andrea Celli
518-436-4691
IMAEC@aol.com

Mary Fangio
315-877-5605
mary@fangiolaw.com

Jessica Grady
315-445-5608
jessica@harrisbankruptcy.com

Paul Levine
518-433-8800
PLevine@lemerygreisler.com

Merritt Locke
315-733-0419
mlocke@saunderskahler.com

Lisa Penpraze
518-434-4553
lisa.penpraze@usdoj.gov

Patrick Radel
315-797-9261
pradel@getnicklivingston.com

Amanda Shaw
315-696-6347
ashaw@riehlmanshafer.com

JoAnn Sternheimer
518-436-0344 x 4926
jsternheimer@deilylawfirm.com

Guy VanBaalen
315-793-8191
guy.a.vanbaalen@usdoj.gov

quality control and reporting purposes. We compare the information on the docket and complaint to the cover sheet to determine the accuracy of the filing. Errors may be corrected or an amendment requested, depending on the error.

Case Administrators are instructed to issue a deficiency notice if the cover sheet is not filed with the complaint. The filer may then file the Adversary Cover sheet as *Adversary > Adversary Miscellaneous > Adversary Cover Sheet*

Free Electronic Noticing for Debtors through the Debtor Bankruptcy Noticing (DeBN) Program coming soon to the New York Northern Bankruptcy Court.

By: Diann Freeman and AnnMarie Waters

Debtor Electronic Bankruptcy Noticing (DeBN) is a FREE and voluntary service that allows debtors to request the delivery of court notices and orders from the bankruptcy court, through the Bankruptcy Noticing Center (BNC), via email instead of the U.S. mail.

The program is available to all debtors with an open bankruptcy case. Debtors can enroll at any time during the pendency of their case. The service requirements for other parties in a bankruptcy case do not change with DeBN.

DeBN offers debtors a number of advantages:

- Debtors receive court notices and orders (e.g., meeting of creditors notice, notice of dismissal, order of discharge, etc.) by email the same day they are filed by the court.
- Debtors can access emailed court notices and orders from a computer or mobile device.
- There is no charge and no limit to the number of times emailed court notices and orders can be viewed.

Information on how to take advantage of this service will be available on the court's website by December 2015.

Application to Have the Chapter 7 Filing Fee Waived

By: Elizabeth Vadney

In lieu of paying the prescribed chapter 7 filing fee or filing an installment application, an individual debtor may, along with the bankruptcy petition, file an application to waive the filing fee. The eligibility requirements are:

1. The debtor(s) has income less than 150 percent of the official poverty line applicable as defined by the Office of Management

Local Rule Standing Committee List Continued:

Richard Weiskopf
518-782-9100
rweiskopf@bwlawpc.com

Jill Dalrymple
315-266-1127
jill_n_dalrymple@nynb.uscourts.gov

Cindy Platt
518-257-1620
cynthia_platt@nynb.uscourts.gov

Dawn Simmons
315-295-1683
dawn_simmons@nynb.uscourts.gov

Beth Vadney
518-257-1615
elizabeth_vadney@nynb.uscourts.gov

Dina Ventura
315-266-1109
dina_ventura@nynb.uscourts.gov

Diann Freeman
315-266-1120
diann_freeman@nynb.uscourts.gov

and Budget; and

2. is unable to pay that fee in installments.

Note: The Judges in the Northern District of New York do have a bright line regarding In Forma Pauperis applications. It is their policy that when an attorney receives payment of counsel fees, the court's filing fee must equally be paid. Thus, in this scenario an application to waive the filing fee would not be granted.

Finally, the court may vacate or revoke an order waiving the filing fee if developments in the case or the administration of the estate demonstrate that the waiver was unwarranted.

Loss Mitigation in 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 1060 Loss Mitigation Requests have been filed and 486 have been concluded. Now that we have lived with this new program for well over two years and have had such an impressive number of requests, the court and bar have noted the need for tweaks and changes to our current practice. The judges requested the establishment of a Loss Mitigation Strategic Planning Committee to propose changes and present them to the judges. In addition, the court sent out a survey to bar members who participate in the program in order to receive feedback to assist the committee in recommending changes.

The committee has been formed. The committee members consist of bar members and court staff. The committee consists of the following members:

Cynthia Platt, Esq.	Patrick Radel, Esq.	Paula Barbarulo, Esq.
Jason Brott, Esq.	William Schiller, Esq.	Elizabeth Vadney
Jill Dalrymple, Esq.	Dawn Simmons, Esq.	Mark Swimelar, Esq.
Andrea Celli, Esq.	Peter Orville, Esq.	

If you need contact information or have any questions please call Cynthia Platt, co-chair, at 518-257-1620

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:

Nicole Smith – Syracuse
AnnMarie Waters – Albany
Daniel Harrigan – Albany
Dana Rosenberg – Albany
Cindy Platt – Albany
Beth Vadney – Albany
Jim Fleming – Utica
Dina McDonald – Albany
Theresa O'Connell – Albany

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

Diann Freeman – 15 Years
Beth Vadney – 20 Years
Jeff Dingman – 25 Years
Kathy Coughlin – 25 Years
Jim Fleming – 25 Years
Judy Bazan – 25 Years

New York Northern Bankruptcy Mediation Program

By: Kim Lefebvre

The Northern District of New York Local Rules at Appendix IV contains the court's Mediation Program. It covers assignment, effect and the procedure for matters ordered to mediation. It also outlines the qualifications, appointment methods, ethical standards, compensation and disclosures required of mediators.

Section 4.2.1 outlines the qualification requirements and application process for an applicant seeking appointment to the Mediator Panel. The application is located on the court's official website at

http://www.nynb.uscourts.gov/sites/default/files/local_rules/NDNY%20Mediator%20Application%204.28.14.pd

Applications must be emailed to mediation@nynb.uscourts.gov. They will be received by the clerk of court and considered by the board of bankruptcy judges at their monthly meeting. The applicant will be notified of the judges' determination in writing.

The current Mediator Panel is posted on the court's website at

http://www.nynb.uscourts.gov/sites/default/files/local_rules/Mediation%20Panelformrev.6.17.15.pdf

They will be received by the clerk of court and considered by the board of bankruptcy judges at their monthly meeting. The applicant will be notified of the judges' determination in writing.

Anyone having an interest in Mediator Panel service should check the court's website or call Kim F. Lefebvre, Clerk of Court at 518-257-1661.

Bankruptcy is about financial death and financial rebirth. Bankruptcy is the great American story rewritten. We're a nation of debtors.

Elizabeth Warren

Bankruptcy represents a longstanding commitment in this country to helping people get a fresh start. This principle has never been giving only certain people a fresh start.

Tim Johnson

High bankruptcy rates, increased credit card debt, and identity theft make it imperative that all of us take an active role in providing financial and economic education during all stages of one's life.

Ruben Hinojosa

When I became CEO of Xerox 10 years ago, the company's situation was dire. Debt was mounting, the stock sinking and bankers were calling. People urged me to declare bankruptcy, but I felt personally responsible for tens of thousands of employees.

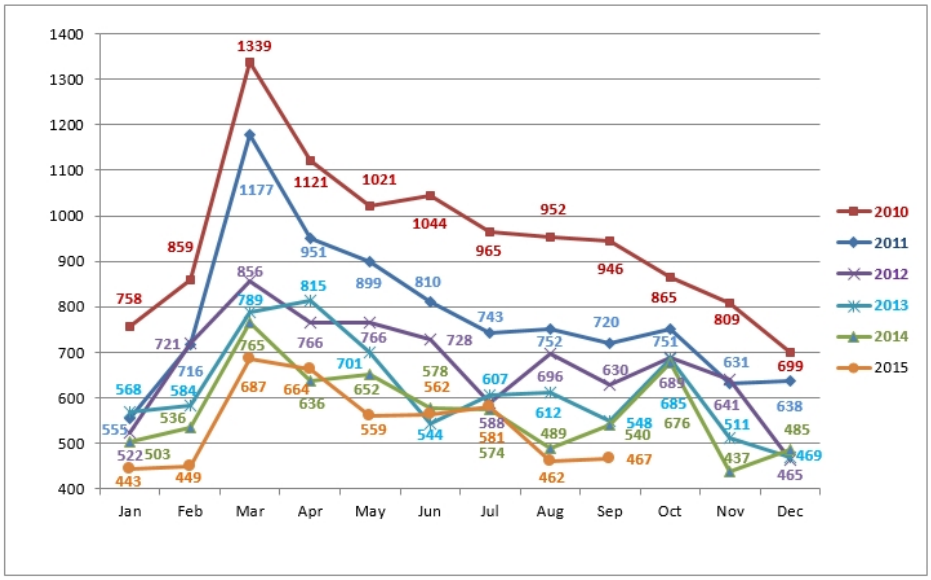
Anne M. Mulcahy

It is said that the world is in a state of bankruptcy, that the world owes the world more than the world can pay.

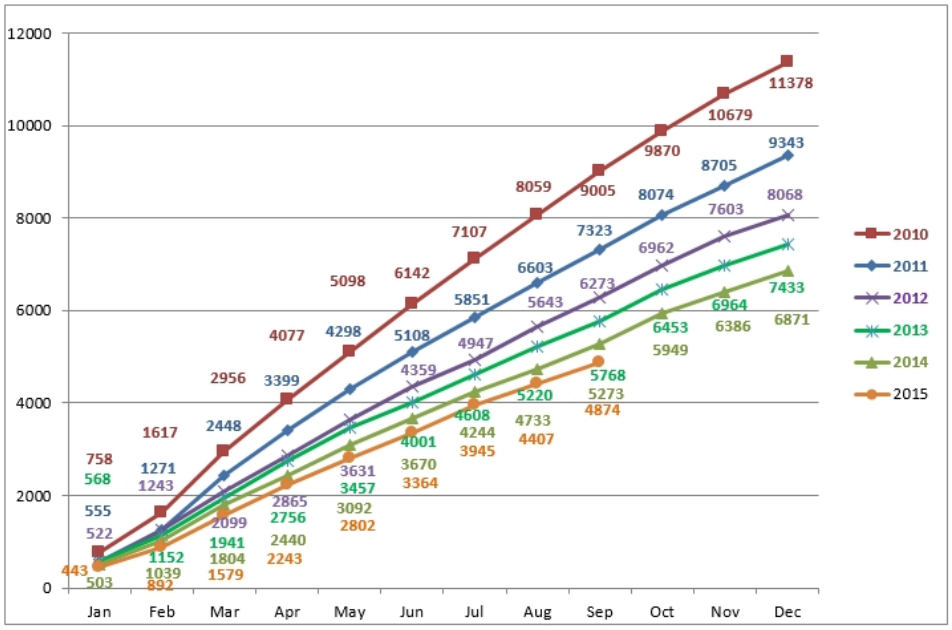
Ralph Waldo Emerson

US Bankruptcy Court NDNY Case Filings Statistics

US Bankruptcy Court NDNY Case Filings by Month 2010-2015



US Bankruptcy Court NDNY Total Filings 2010-2015



Cybersecurity and the Protection of Client Information

by James E. Fleming, Systems Manager

The relationship between an attorney and a client is one built on trust. A client believes that the confidences entrusted to his/her attorney are to be used only in furtherance of enforcing or protecting the client's rights and privileges under the law. This trust is codified in the "Rules of Professional Conduct" effective in New York State: "A lawyer shall not knowingly reveal confidential information […] or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person," subject to specific exceptions.[1] The obligation placed upon an attorney to "not knowingly reveal confidential information" may possibly be replaced by a stricter standard in the near future.

We live in an era in which desktop pcs and laptops have become standard equipment for white-collar workers. Data is increasingly stored in "the cloud" rather than in a filing cabinet. Attorneys and law firms conducting business with the federal courts now do so by filing digitized documents in an electronic file format rather than in paper form. But is confidential information provided by a client, once preserved on paper and stored in an attorney's safe or locked filing cabinet, as secure today when preserved on a pc, mobile electronic device or server? To what degree is an attorney responsible for protecting a client's confidential information from computer hackers and thieves? Should a client be allowed a reasonable expectation that his/her confidential information will be protected from cyberthreats while in an attorney's possession?

In an interview for a September 2014 newspaper article, an FBI agent succinctly stated, "Computer attacks on law firms happen every day…."[2] Attorneys and law firms "are perceived as easy targets for attacks."[3] Attorneys possess specific information relating to specific matters affecting their clients. "[L]lawyers are usually involved in only their client's most important business matters, meaning hackers may not need to sift through extraneous data to find the more valuable information."[4]

---

[1] "New York Rules of Professional Conduct", Rule 1.6(a); effective April 1, 2009, as amended through December 20, 2012, with commentary as amended through March 28, 2015.

[2] Andrew Conte, *Unprepared Law Firms Vulnerable to Hackers*, TribLive, Sept. 13, 2014 (available at http://triblive.com/news/alleghany/6721544-74/law-firms-information#axzz3TuTnls4O).

[3] Drew Simshaw and Stephen S. Wu, *Ethics and Cybersecurity: Obligations to Protect Client Data*, American Bar Association Section of Labor & Employment presentation at the National Symposium on Technology in Labor and Employment Law, San Francisco, CA, March 15-17, 2015 (available at http://www.americanbar.org/content/dam/aba/events/labor_law/2015/march/tech/wu_cybersecurity.authcheckdam.pdf).

[4] Jane LeClair & Gregory Keeley, *Cybersecurity in Our Digital Lives*, A Volume in the Excelsior College Press Series "Protecting Our Future", Hudson Whitman Excelsior College Press (2015), page 128.

Attorneys possess large amounts of information that could be valuable to both state and non-state attackers. A law firm representing a corporate client may be a target of an attacker trying to obtain the client's trade secrets. An attacker may also seek to obtain the identity of a corporation's potential acquisition targets in order to profit from stock trades. An attacker may view an attorney or law firm as an easy target for the purpose of obtaining clients' personal information to be used for identity theft purposes or even blackmail.

As a result, it is becoming increasingly clear that an attorney has some degree of responsibility to protect a client's confidential information from a cyberattack. The American Bar Association's Model Rules of Professional Conduct state "[a]A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[5] Most states have adopted similar provisions. In 2010, the State Bar of California went a step further when considering "a matter in which an attorney used his personal laptop to work on a client's information from home; access a pubic Wi-Fi network to conduct legal research for the client's matter; and communicate via email with the client while away from the office."[6] Having considered the issue in the context of the attorney's duty of competence, the California Bar concluded

> "[a]An attorney's duties to confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representation does not subject confidential client information to an undue risk of unauthorized disclosure. Because of the evolving nature of technology and differences in security features that are available, the attorney must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps."[7]

The Connecticut Bar Association, in Informal Opinion 2013-07, also weighed in on an attorney's duty of competence when it stated

> "[t]The privilege of practicing law comes with professional obligations and those obligations extend to the use of technology. Rule 1.1 [of the CBA Rules of Professional Conduct] Official Commentary…expressly provides that in order 'to maintain the requisite knowledge and skill, a lawyer should keep abreast of

[5] American Bar Association, *Model Rules of Professional Conduct*, Rule 1.6(c) (available at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html).
[6] Joseph M. Burton, 4 Steps to Getting Serious About Law Firm Cybersecurity, Law Practice Today, Sept. 15, 2014 (available at http://www.lawpracticetoday.org/article/4-steps-getting-serious-law-firm-cybersecurity/).
[7] *Id.*

> changes in the law and its practice, including the benefits and risks associated with relevant technology…."[8]

The Connecticut Bar Association continued on by addressing an attorney's duty of confidentiality:

> "Rule 1.6 of the [CBA] Rules of Professional Conduct governs the confidentiality of client information. In relevant part, Rule 1.6(a) provides that 'a lawyer shall not reveal confidential information relating to the representation of a client unless the client consents after consultation….' The duty of confidentiality imposed by Rule 1.6(e)…requires a lawyer to avoid using means or methods of holding and delivering data that present an unreasonable risk of unintended disclosure to and access by unauthorized third parties."[9]

In Ethics Opinion 1019, the New York State Bar Association discussed cybersecurity in the context of confidentiality and remote access to a law firm's electronic files. In particular, the Bar Association's Committee on Professional Ethics stated

> "Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks…. In light of these developments, it is even more important for a law firm to determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected…. If the firm cannot conclude that its security precautions are reasonable, then it may request the informed consent of the client to its security precautions, as long as the firm discloses the risks the system does not provide reasonable assurance of confidentiality, so that the consent if "informed" within the meaning of [NYS Bar Association Rule of Professional Conduct] Rule 1.0(j)."[10]

The Committee's conclusion in Ethics Opinion 1019 is in keeping with the conclusions reached in the above-mentioned opinions of the California and Connecticut Bar Associations: an attorney has a duty to keep client information confidential; the duty extends to using appropriate security to protect the information contained in electronic files; and an attorney has a duty to request the informed consent of his/her client to the security precautions should the attorney be unable to conclude that the security precautions are reasonable.

---

[8] Connecticut Bar Association, *Informal Opinion 2013-07, Cloud Computing*, approved June 19, 2013 (available at http://c.ymcdn.com/sites/ctbar.site-ym.com/resource/resmgr/Ethics_Opinions/Informal_Opinion_2013-07.pdf).
[9] *Id.*
[10] New York State Bar Association, *Ethics Opinion 1019*, Aug. 8, 2014 (available at https://www.nysba.org/CustomTemplates/Content.aspx?id=51308).

Recently, a number of leading law firms, under pressure from major financial institutions and high profile corporate clients, have begun to take a proactive approach to cybersecurity and the protection of client information. A growing number of Am Law 200[11] law firms have obtained or are in the process of obtaining certification showing that their information security management systems meet the ISO 27001 international cybersecurity standard. A handful of Am Law 100 and U.K. firms are also "working to form an alliance that would allow them to ultimately share information with each other about cyberthreats and vulnerability." These initiatives are being undertaken by law firms with the revenue and resources to invest in such undertakings. The question remains: what can relatively small law firms and individual attorneys do to protect client information from cyberthreats?

Below is a list of steps you can take to best protect the confidential information entrusted to you by your clients:

1. Hire a reputable Information Technology business specializing in cybersecurity to manage and maintain the security of your systems and software;
2. Become 'cyber savvy': receive basic cybersecurity awareness training at least once a year. Many bar associations offer some form of cybersecurity training;
3. Read! The internet contains a wealth of information related to cyberthreats and how best to prevent them;
4. Never use operating systems or software that are no longer supported by their developers (ex.: Microsoft Windows 95, 98, and XP);
5. If planning on implementing a third-party cloud storage solution, perform due diligence. The American Bar Association provides cloud-computing guidance for attorneys.[12]
6. Install antivirus/antimalware software on all office pcs and laptops, make sure virus definition files are automatically updated at least once a week, and schedule weekly full system virus scans of the pcs and laptops;
7. Install a firewall on all office pcs and laptops;
8. Check for operating system and software updates on all pcs, laptops, and mobile computing devices such as smartphones and tablets once a week; install updates as they become available.
9. Only use work pcs, laptops, and mobile computing devices for work-related business. Do not read personal email, visit websites unrelated to work, or install unnecessary software or apps on office systems;
10. If you have any reason to believe an email may be suspicious, do not open it;

[11] The "Am Law 100" and "Am Law 200" are rankings compiled by American Lawyer magazine of U.S. law firms with the highest annual gross revenue.

[12] YourABA Newsletter, "Evaluating cloud-computing providers", June 2012 (available at http://www.americanbar.org/content/newsletter/publications/youraba/201206article12.html)

11. Be conscientious of the information you post on social media websites such as Facebook, Twitter, LinkedIn, etc., as these websites provide hackers and cyberthieves with a wealth of information about potential targets;
12. Create an incident response plan that can be easily followed should you discover a breach of your systems has occurred. The Department of Justice's document entitled "Best Practices for Victim Response and Reporting Cyber Incidents"[13] provides guidance on the steps that should be taken in response to a cyberattack.
13. Report a suspected cyberattack to the FBI by contacting the office located nearest to you. The FBI offices located in New York State are listed in the table below:

Office	Address	Phone Number
FBI Albany	200 McCarty Avenue Albany, NY 12209	(518) 465-7551
FBI Buffalo	One FBI Plaza Buffalo, NY 14202-2698	(716) 856-7800
FBI New York	26 Federal Plaza, 23rd Floor New York, NY 10278-0004	(212) 384-1000

[13] Department of Justice, "Best Practices for Victim Response and Reporting of Cyber Incidents", Version 1.0, April 2015 (available at http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf).

Drive-By Download Attacks: What They Are and How They Can Be Avoided

by James E. Fleming, Systems Manager

What is a drive-by download attack?

A drive-by download is a type of cyber attack in which a person visits a legitimate website that has been compromised by hackers. The person's computer is either directly infected with malware or becomes infected after the browser has been redirected to a malicious site. A drive-by download attack can also be perpetrated by luring a person to click on a pop-up or malicious ad embedded on a legitimate website resulting in the browser being redirected to a malicious site.

What type of malware is distributed by a drive-by download attack?

Drive-by download attacks have been used over the years to infect the computers of its victims with a wide range of malware including viruses, spyware, keyloggers, and remote-access programs. However, drive-by download attacks have increasingly become the method used by hackers to install banking trojans and ransomware on its victims' computers. A banking trojan is used to steal the victim's online banking credentials, allowing the hackers to hijack the victim's account. Ransomware encrypts files on the victim's computer, then demands a ransom from the victim in return for unlocking the files. Payment of the ransom does not ensure that the hacker will actually provide the means to unlock the files.

What types of web sites are most at risk?

Hackers prefer to use well-established, popular, high-traffic web sites as the launch pad for their drive-by download attacks. In the past, the web sites of the New York Times, NBC, Google, and Microsoft have been compromised by hackers in order to initiate the attacks. Popular pornography and file sharing sites are also commonly used.

How can you protect yourself?

- Install updates for your operating system (e.g.: Microsoft Windows, Apple OS X, Apple iOS, etc.) soon after they have been released.
- Regularly check for patches and updates to web browsers (e.g.: Internet Explorer, Firefox, Chrome, Safari) and key programs (e.g.: Adobe Flash Player, Adobe Reader, Java, etc.).
- Run an anti-virus program on your computer at least once a week; either configure the program to install virus definition updates automatically, or manually install the updates a minimum of once a week.
- Regularly update and run a malware detection program on your computer.
- Install a firewall on your computer.

- Consider running a script-blocking web browser plugin such as Adware Plus, ScriptSafe, or NoScript[1] to block popups, advertising content, and malicious scripts embedded in websites.
- Frequently back up your data to an external hard drive or device; disconnect the external hard drive from your computer once the backup has completed.
- Do not store your logins and passwords in a file on your computer; if you can access the file, so can hackers.
- If possible, do not log into online banking accounts from a computer used to surf the web; use a computer dedicated to online banking only.

[1] Reference to AdBlock Plus, ScriptSafe, and NoScript does not constitute an endorsement of these programs by the United States Bankruptcy Court for the Northern District of New York.

Beware of Phishing Scams

by James E. Fleming, Systems Manager

What Is a Phishing Scam?

More than 200 billion emails are sent and received worldwide every day.[1] Of that enormous number, an increasing percentage fall into the category of phishing scams. "Phishing" is a scam in which scammers send emails that appear to originate from legitimate organizations or individuals, and try to entice the recipients into clicking on malicious links or attachments. "Spear-phishing" is a form of phishing that targets specific individuals or organizations. While spear-phishing attacks can be an attempt by the scammer to steal trade secrets, both phishing and spear-phishing attacks are often used to steal financial information or sensitive information later used to commit fraud. Phishing can also be used as a method to gain access to an organization's network for cyber espionage or to create a platform for further malicious activity.

As a means of gaining the trust of potential victims, scammers will use spoofed email addresses, phony websites with legitimate logos, or phone numbers to fake service centers operated by the scammers. It is estimated that phishing attacks cost organizations $4.5 billion dollars in losses during 2014.[2]

How to Recognize a Phishing Scam

Years ago, it was relatively easy to recognize a phishing email by the poor syntax used in its body. The recipient of the email was often referred to as "dear esteemed friend" rather than by the more common "dear customer" or "dear account holder." Over the years, scammers have become craftier at creating convincing phishing emails. However, you can minimize your risk of falling victim to scammers by looking for the following potential phishing traps and telltale signs of a scam:

- An email purporting to be from a bank, credit card company, or other financial institution claims that your account information has been lost or your account is going to be closed. The email conveys a sense of urgency and may even contain the word "urgent" in the subject field or body. You are asked to "confirm" your personal account information by calling the provided phone number or clicking a link within the email.
- An email purportedly from the "fraud department" of a well-known company states you may be the victim of identity theft and asks you to verify your personal information.
- An email claiming to be from a state of foreign lottery commission requests your banking information in order to "deposit the winnings" into your accounts.
- A scammer claims to have a large sum of money and needs help accessing it. The scammer indicates that he has contacted you because of your

[1] http://www.radicati.com/wp/wp-content/uplods/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf
[2] http://www.emc.com/emc-plus/rsa-though-leadership/online-fraud/index.htm

trustworthiness, and promises to share a portion of the money with you in exchange for your assistance. You are asked to provide your financial information.
- An email related to a current event (e.g., the Anthem or Target data breach) and containing malicious links to "free credit reporting."

Easy Ways to Protect Yourself from Phishing

The following are easy ways to protect yourself from becoming a victim of a phishing scam:

- Do not send any sensitive personal information via email. Legitimate organizations will not ask uses to send information in this manner.
- Visit a banking or financial website by typing its internet address (also known as a "URL") directly into your browser's address bar. Do not follow links embedded in unsolicited email.
- Do not open an email attachment if you weren't expecting to receive it or are unsure of what it contains. Be cautious of container files, such as .zip files, as malicious files could be packed inside.
- If you would like to verify a suspicious email, contact the organization directly. However, do not call any phone number that is provided within the email.
- Use discretion when posting personal information to social media sites. Spear-phishing scammers often gather information found at such sites to create emails that appear to be trustworthy.
- Use antivirus and antimalware software to detect and remove malicious programs, such as spyware or backdoor Trojans, which may be included in phishing email. Keep your operating system, Internet browser, and software such as Adobe Acrobat Reader and Adobe Flash updated with the latest security patches.

Helpful Links

- Anti-Phishing Working Group: http://www.antiphishing.org
- Internet Crime Complaint Center (IC3): http://www.ic3.gov/default.aspx
- Federal Trade Commission: https://www.consumer.ftc.gov/articles/0003-phishing