THE SUFFOLK LAWYER

THE OFFICIAL PUBLICATION OF THE SUFFOLK COUNTY BAR ASSOCIATION

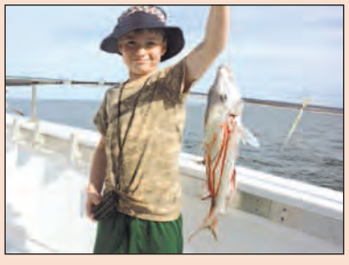
DEDICATED TO LEGAL EXCELLENCE SINCE 1908 www.scba.org Vol. 33, No. 1 – September 2017

INSIDE

SEPTEMBER 2017 FOCUS ON CYBERSECURITY

Nationwide data breach lawsuit 10
Responding to a cybersecurity breach ...9
Cybersecurity due diligence 10
Cybersecurity in healthcare 11

Dean's List 6
Pro Bono attorneys celebrated 16
Unsung Heroes 3
Meet Your SCBA Colleague 3
Book review 12



SCBA happenings 21

Legal Articles

ADR 19
Bench Briefs.....4
Constitution 19
Consumer Bankruptcy.....20
Court Notes 8
Cyber 20
Ethics.....6
Family.....12
Inside the Courts 4
LGBT 5
Personal Injury – Devlin 14
Personal Injury – Donaldson.....8
Real Estate 13
Trial Practice 14
Trusts and Estates.....15
Who's Your Expert.....18

Among Us 7
CLE Course Listings.....30
Freeze Frame 25, 28
SCBA Calendar 2

Another great SCBA Annual Outing

Photo by Barry Smolowitz

More people than ever before attended this year's SCBA Annual Outing enjoying a day of fishing or a day of golf. See more photos on page 21.

By Sarah Jane LaCova

The morning dawned on our Annual Outing on Monday, August 14 bringing us a mixture of sun and clouds. Despite overcast skies, a record number of members and guests participated enthusiastically in the day's sporting events and enjoyed a sumptuous feast of lobsters, shrimp, clams, steak (to name but a few of the special dishes and delicacies) as the piece de resistance in the early evening at the Rock Hill Country Club in Manorville.

Kudos to Barry Smolowitz, who accompanied the stalwart band of fishing devotees out on Port Jefferson harbor aboard the Osprey, a private charter fishing boat owned by the Cash family. Thank you to the sponsors of the fishing trip Carr Business Systems, Barry

(Continued on page 28)

PRESIDENT'S MESSAGE

The Value of SCBA Committee Membership

Pat Meisenheimer

By Patricia Meisenheimer

Serving on a committee offers the opportunity to build a network of valuable professional contacts and friendships, both within your practice or interest area and outside your day-to-day practice. The Suffolk County Bar Association Committees provide its membership with opportunities to improve their professional skill and knowledge, strengthen the administration of justice, keep members informed of significant developments in their area of practice and shape association policy on issues of professional concern.

Active participation in the work of the SCBA gives unparalleled opportunities to meet and get to know other outstanding attorneys. Involvement enriches our professional lives, gives us the opportunity to work together to improve the law, the profession and address crucial problems facing the legal system. Committees provide the opportunity for problem solving and can be a forum for presenting multiple points of view. Committees are the training ground for future leadership and provide a forum for leaders to refine their skills and abilities. Committees are the operating system of our Association, involving our members in the development and delivery of member needs by collective decision making.

(Continued on page 22)

BAR EVENTS

Annual Judiciary Night

Wednesday, Oct. 18, at 6 p.m.
U.S. Federal Courthouse, Central Islip

We will be paying tribute to our Appellate Justices Hon. Sandra L. Sgroi and Hector D. LaSalle. Cost: $60/person.

Annual Halloween Party

Friday, Oct. 27 at 6 p.m.
Great Hall, Bar Center

The Charity Foundation will host this popular event for the second time. Come in costume and get a raffle ticket. Meet Freddie the Dragon, and Edith, who reads Tarot Cards, and Witchy Poo. There will be skeletons and jack-o-lanterns and lots of fun. Look for the flyer on our website.

FOCUS ON CYBERSECURITY
SPECIAL EDITION

CYBER

Confidentiality requires cybersecurity

By Victor Yannacone, Jr.

Disciplinary Rule 1.6(a) provides that "A lawyer shall not knowingly reveal confidential information…" The rule further defines "Confidential information" as "information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential . . ." whether the client is a current client, a former client (Rule 1.9(c) or even a prospective, but not yet retained client (Rule 1.18(b).

The recently promulgated Rule 1.6(c) imposes a non-delegable duty and affirmative obligation upon an attorney t0 "make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b)."

According to Rules 1.1, 5.1 and 5.3, attorneys must safeguard confidential information against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the attorney or other persons who are participating in the representation of the client or who are otherwise subject to supervision by the attorney. That includes any vendors or employees of vendors involved in litigation support, particularly e-discovery.

Duty to preserve confidentiality

The burden is upon the attorney to make reasonable efforts to prevent unauthorized access to or disclosure of information protected by Rules 1.6, 1.9, or 1.18.

The reasonableness of the cybersecurity efforts an attorney makes to protect client confidential information is always determined after some disclosure of client confidential information has occurred.

The extent to which the attorney will be held liable and responsible for the unauthorized access or disclosure will depend upon a number of factors including the sensitivity of the information; the probability of disclosure because certain available safeguards and cybersecurity measures were not employed; the cost of those safeguards and cybersecurity measures; the difficulty of implementing the safeguards and cybersecurity measures, which might have been reasonably expected to have prevented the unauthorized access or disclosure; and in certain cases the extent to which the safeguards and cybersecurity measures might have adversely affected the ability of the attorney to represent the client. This latter "defense" becomes important in litigation with extensive discovery, intellectual property matters, and cases involving handling of records subject to HIPAA (Health Insurance Portability & Accounting Act) mandates.

Victor Yannacone

Today, many clients with established IT (Information Technology) departments require their attorneys to implement the same cybersecurity measures the company implements. Attorneys should try to obtain informed consent from their client to accept the security measures which the attorney has already established.

Attorneys are vulnerable to being charged with a violation of Rule 1.6(c) when transmitting confidential information in some kind of electronic format, particularly as an e-mail attachment. The attorney must take reasonable precautions to prevent the information from reaching unintended recipients. A mere "expectation" of confidentiality is not enough.

Rule 1.6(c) creates new risks for attorneys

Law firms hold vast collections of sensitive client documents — data of significant value to hackers. Law firm hacking is now pervasive.

Many law firms do not require any security on mobile devices — laptops, tablets, and smart phones. Mandatory password protection, encryption, and remote wiping capability should be the bare minimum security for these devices.

E-discovery increases the potential exposure of any attorney to liability if there are not sufficient safeguards in place and sound cybersecurity practices have not been implemented. The probability of inadvertently producing privileged and confidential documents increases with each gigabyte.

Law firms from the smallest to the largest, and even solo practitioners should consider adopting security mechanisms such as data loss protection ("DLP") systems, also known as data leak prevention systems, to help detect and prevent the potential unauthorized or inadvertent transmittal of confidential information by employees. DLP systems classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure might violate Rule 1.6(c).

Various federal laws impose affirmative obligations on law firms to protect certain categories of information in their possession, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Fair and Accurate Credit Transactions Act of 2003 (FACTA), the Gramm-Leach-Bliley Act (GLBA), and others. However, Rule 1.6(c) goes far beyond the specifics of these statutes.

Encrypt everything!

Encryption, including file encryption, e-mail encryption and full-disk encryption, represents a relatively simple and effective risk management tool. The use of full disk encryption on laptops and other mobile devices can help mitigate the risk if the device is lost or stolen because the information will not be accessible to anyone without the key.

Use caution in the cloud

When a lawyer stores firm and client information in the cloud, that information is essentially stored off site, possibly in another country where it may be subject to international search and seizure laws.

Wisdom and prudence suggest that an attorney should obtain written consent from a client before storing their confidential information in the cloud. It is also important to know whether the information stored in the cloud will be encrypted end to end.

Note: Victor John Yannacone Jr. is an advocate, trial lawyer, and litigator practicing today in the manner of a British barrister by serving of counsel to attorneys and law firms locally and throughout the United States in complex matters. Mr. Yannacone has been continuously involved in computer science since the days of the first transistors in 1955 and actively involved in design, development, and management of relational databases. He pioneered in the development of environmental systems science and was a cofounder of the Environmental Defense Fund. He can be reached at (631) 475–0231, or vyannacone@yannalaw.com, and through his website https://yannalaw.com.

CONSUMER BANKRUPTCY

Chap 13 Debtors Must Be Current at Time of Discharge

By Craig D. Robins

This summer saw two decisions handed down by our judges in the Central Islip Bankruptcy Court that will make it harder for some struggling Chapter 13 debtors with mortgages to obtain their discharges.

Most consumers seek Chapter 13 relief to utilize the Chapter 13 payment plan to cure mortgage arrears over a sixty-month period, stopping any foreclosure proceeding in the process. The plan also enables the debtor to discharge credit card debt by often paying just pennies on the dollar.

The plan requires the debtor to pay the current monthly mortgage payment "outside the plan" directly to the mortgagee, while satisfying the arrears with monthly plan payments to the trustee.

For years, many debtors entering the home stretch of their plan would find themselves struggling to make all necessary payments including remaining current on their post-petition mortgage payments. Their attorneys would suggest that if they didn't have enough money, they should just make the trustee plan payments, get their discharge, and then enter into a payment arrangement with the mortgagee. However, that approach is now history.

Craig Robins

Both Judge Alan S. Trust and Robert E. Grossman have held that if a Chapter 13 debtor is not current with the post-petition mortgage payments when the plan ends, he or she is not entitled to a discharge. *In re Coughlin*, 568 B.R. 461(Bankr. E.D.N.Y. Case No.11-76202-ast, June 15, 2007, Judge Trust); *In re Hanley* (Bankr. E.D.N.Y. Case No.11-76700-reg, August 11, 2007, Judge Grossman).

What has happened over the past few years to trigger this? The answer has to do with Bankruptcy Rule 3002.1, a relatively new statute that went into effect in 2011. This statute requires mortgagees to make certain disclosures to increase the transparency of mortgage servicing practices in Chapter 13 cases. It is also designed to prevent post-discharge disputes between debtors and mortgagees with regard to pre-discharge defaults. (This statute was discussed at length in the February 2017 installment of this column, *Mortgagee Sanctioned $375k for Chapter 13 Rule Violation*).

Of importance here, at the end of a Chapter 13 case, the mortgagee must file a "Response to Notice of Final Cure Payment" indicating whether the debtor is cur-

(Continued on page 27)