FEDERAL BAR ASSOCIATION SOUTHERN DISTRICT OF NEW YORK CHAPTER

Fall 2015 The Newsletter of the Southern District of New York Chapter of the FBA

IN THIS EDITION

Letter from the President

Welcome Southern District of New York Chapter members. As incoming chapter president for 2015-2016, I am honored to represent the chapter at such an exciting time. In 2018, our chapter will host the Federal Bar Association's National Meeting and Convention here in New York, and the planning committee has already begun planning a phenomenal and memorable convention.

This year, the chapter has many events and opportunities to connect with fellow lawyers and our federal judiciary. Please join us on October 6, 2015 at 5:00 p.m. for the swearing-in of SDNY chapter officers and directors. We are honored to have the Hon. Loretta A. Preska, Chief Judge, SDNY, presiding over the ceremony, and we graciously welcome the Hon. Frank Maas, Chief Magistrate Judge, SDNY, as a new member of the chapter's board of directors.

We also have a number of exciting programs planned for this year. On October 20, please join us for an all-day Securities Law and AML Conference and CLE, featuring a highly distinguished panel of attorneys and regulators. We are fortunate to have Chief Judge Preska as the featured speaker during the luncheon. Additionally, Chief Judge Preska is traveling to Washington, D.C. for the Federal Litigation Conference on October 27. I encourage you all to attend this event.

The chapter's Immigration Law committee and national Immigration Section are hosting Asylum Day, an all-day event at Benjamin N. Cardozo School of Law on November 16. This event will also feature amazing speakers and be a fascinating and unique program.

On January 21, 2016, we are hosting our annual Rule of Law event, honoring Bryan Stevenson of the Equal Justice Initiative. We also invite you to join us for upcoming events honoring women in the law, our military and the U.S. Marshal for SDNY. Promotional brochures will be circulated when dates are announced.

In this edition of New York Minutes, you will find fascinating articles on agent designations under the Digital Millennium Copyright Act, by J. Brugh Lower, developing cybersecurity plans in an age of hacking and cyber espionage, with an eye toward litigation, in an article by Jason E. Glass, and the expansion of liability for retaliation under the Fair Labor Standards Act, by Saranicole A. Duaban.

Please contact the editors if you would like to contribute an article to the New York Minutes, and feel free to contact me at MZussman@cdas.com for more details about any of our upcoming events and other information about the chapter.

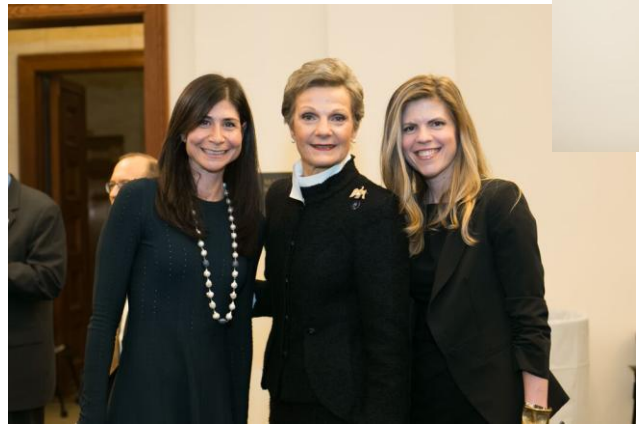
-Michael J. Zussman

SDNY Chapter Events

Meet the Chiefs

Chief Magistrate Judge Frank Maas, S.D.N.Y.

March, 2015

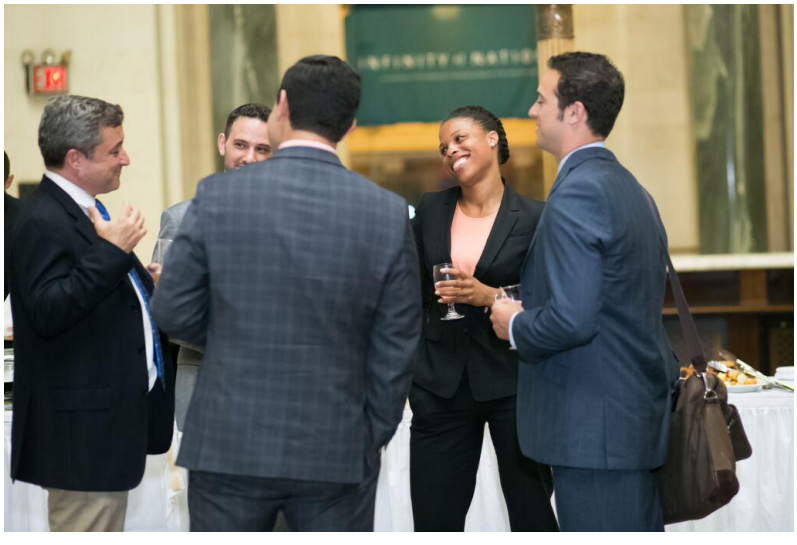


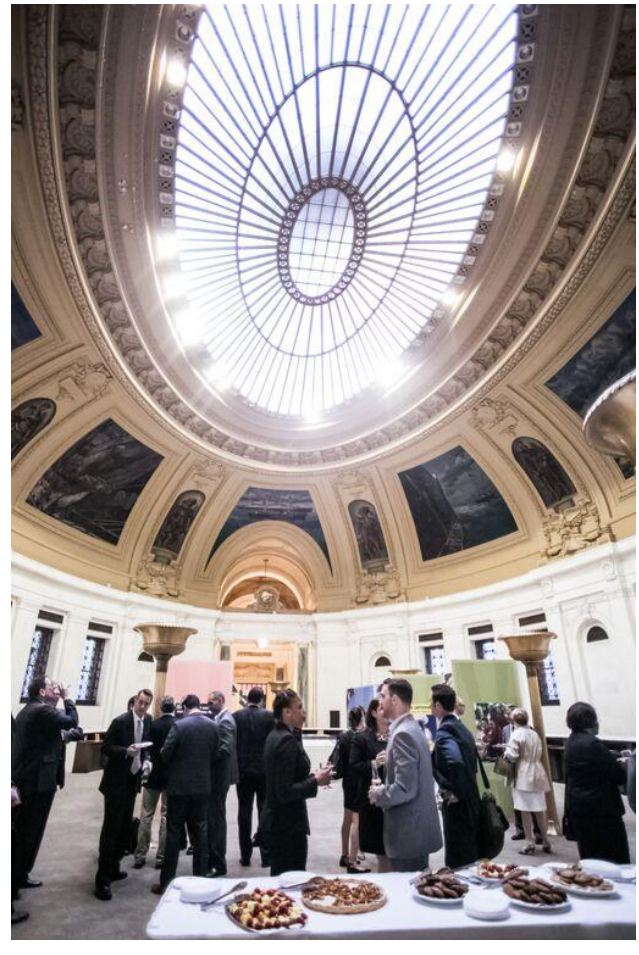
(L-R) Danielle Lesser, Chief Judge Loretta A. Preska, Olivera Medenica

Chief Judge Robert A. Katzmann, United States Court of Appeals for the Second Circuit

SDNY Bankruptcy Event

June, 2015





Recent S.D.N.Y. Decision Provides Guidance Concerning DMCA Agent Designations

By J. Brugh Lower, Esq.

A recent S.D.N.Y. decision should be closely read by online service providers that seek safe harbor from copyright infringement claims under the Digital Millennium Copyright Act ("DMCA"). In *BWP Media USA Inc. v. Hollywood Fan Sites LLC*, No. 14-CV-121, 2015 WL 3971750 (S.D.N.Y. June 30, 2015), Judge Oetken of the Southern District of New York ruled that the defendant online service providers were not entitled to safe harbor under the DMCA because (1) safe harbor does not extend to infringement that occurred prior to a proper DMCA agent designation; (2) a DMCA agent designation by a parent corporation on behalf of "subsidiaries and affiliates" did not extend safe harbor to unnamed subsidiaries and affiliates; and (3) specifying an agent on a corporate website without registration with the Copyright Office is not an effective DMCA agent designation.

A. Background of DMCA Safe Harbor Provisions

Congress enacted the DMCA in order to update copyright law for the digital age. Recognizing the potential for online service providers to be exposed to copyright infringement claims in connection with data residing on their systems or networks as a result of users, Congress added four safe harbor provisions to the Copyright Act that, under certain circumstances, shield service providers from copyright infringement liability. In order to receive protection under the safe harbors, a party must meet certain threshold criteria—namely, it must qualify as a "service provider" as defined in the statute, have adopted and reasonably implemented a "repeat infringer policy," and accommodate "standard technical measures" used by copyright owners to protect copyrighted works. *Id.* at *3 (quoting *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 27 (2d Cir. 2012)); *see* 17 U.S.C. § 512(k)(1)(B), (i)(1)(A)-(B), (i)(2).

Once those initial requirements have been satisfied, an online service provider must also satisfy the requirements of one of the four safe harbor provisions codified at 17 U.S.C. § 512(a) through § 512(d). *See Hollywood Fan Sites*, 2015 WL 3971750, at *3. The safe harbor provision at § 512(c), the provision implicated in *Hollywood Fan Sites*, covers infringement claims that arise "by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider." 17 U.S.C. § 512(c)(1). One of the requirements under § 512(c) is that the service provider "designate[] an agent to receive notifications of claimed infringement." *Id.* § 512(c)(2). In order to make a proper designation, a service provider must "mak[e] available through its service, including on its website in a location accessible to the public, . . . substantially . . . the name, address, phone number, and electronic mail address of the agent," as well as "other contact information which the Register of Copyrights may deem appropriate." *Id.* The statute also requires that the same information be provided to the U.S. Copyright Office ("USCO"), which maintains a public online directory of DMCA agents. *Id.* The agent designation and filing with the USCO provides copyright holders a way to easily find and notify service providers of any claims of copyright infringement.

B. *Hollywood Fan Sites* Decision

In *Hollywood Fan Sites*, Plaintiffs BWP Media USA Inc., National Photo Group, LLC, and Fameflynet, Inc. ("Plaintiffs") filed a lawsuit in the Southern District of New York against Hollywood.com, LLC ("Hollywood") and two of its subsidiaries, Hollywood Fan Sites LLC ("HFS") and Fan Sites Org, LLC ("FSO") (collectively, "Defendants"), for copyright infringement. Plaintiffs alleged that they owned rights to certain celebrity photographs that appeared on websites operated by Defendants without a license and in violation of Plaintiffs' copyrights. In response, Defendants asserted the affirmative defense that Plaintiffs' claims were barred by the safe harbor provisions of the DMCA. Plaintiffs moved for partial summary judgment seeking to strike Defendants' safe harbor defense. Plaintiffs contended that Defendants did not qualify for safe harbor protection because no agent was designated for DMCA notifications at the time of the infringements alleged in Plaintiffs' complaint. The Court granted in part and denied in part Plaintiffs' motion, providing guidance as to the DMCA agent designation requirement under § 512(c).

1. The § 512(c) safe harbor does not extend to acts of infringement that occur prior to the date of the DMCA agent designation.

At the time Plaintiffs filed their complaint against Defendants, each of the Defendants had properly filed a DMCA agent designation. Important to the court's decision in granting Plaintiffs' motion in part, however, was the holding that "[a] service provider cannot retroactively qualify for the safe harbor for infringements occurring before the proper designation of an agent under the statute." *Hollywood Fan Sites*, 2015 WL 3971750, at *3. In reaching that conclusion, the court relied on the express language of the DMCA, which provides that the "[t]he limitations on liability . . . apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement." 17 U.S.C. § 512(c)(2). The court also relied on a recent decision from the Northern District of California, *Oppenheimer v. Allvoices, Inc.*, No. C 14-00499, 2014 WL 2604033 (N.D. Cal. June 10, 2014), that also expressly addressed this issue. There, the court concluded that because § 512(c) "'plainly specifies that a registered agent is a predicate, express condition" that must be met for safe harbor to apply, a party "may not invoke the safe harbor . . . with respect to infringing conduct that occurred prior to . . . designating a DMCA-related agent." *Oppenheimer*, 2014 WL 2604033, at *5.

For those reasons, the court in *Hollywood Fan Sites* held that the defendants FSO and HFS, which had first filed their own DMCA agent designations on November 5, 2012, and December 5, 2013, respectively, could not utilize those designations to implicate the DMCA safe harbor for infringements prior to those dates. The court, however, denied Plaintiffs' motion for summary judgment as to any infringement that occurred after those agent designations, finding that HFS and FSO could still be entitled to safe harbor for any such infringement.

2. A parent company's DMCA agent designation on behalf of "subsidiaries and affiliates" does not extend the § 512(c) safe harbor to unnamed subsidiaries or affiliates.

In addition to its own agent designation, HFS also attempted to rely on a DMCA agent designation filed much earlier by its parent company, Hollywood. Defendants claimed that Hollywood filed that designation on November 3, 2008 "on behalf of and its subsidiaries and affiliates," and that HFS was entitled to safe harbor under § 512(c) by way of Hollywood's designation.

The court disagreed, reasoning that the Hollywood designation made no express reference to HFS and, moreover, that HFS was not specifically listed in the USCO directory at the time. The court concluded that "the statute does not contemplate that a service provider entity can be shielded by the safe harbor where that entity has no presence at all in the USCO directory." *Hollywood Fan Sites*, 2015 WL 3971750, at *5. The Court found it unreasonable to expect "parties attempting to find a provider's DMCA agent designation . . . to have independent knowledge of the corporate structure of a particular service provider." *Id.* Accordingly, the court held that Hollywood's designation could not serve as a basis for HFS's safe harbor defense.

Although the court's holding on this point turned on the failure of the Hollywood designation to specifically refer to HFS, the court went on to reason that even if the Hollywood designation expressly stated that it included HFS, that might still be insufficient because "it is far from clear that a single designation can cover multiple entities." *Id.* The court examined the interim regulations promulgated by the USCO with respect to DMCA designations and concluded that they "explicitly reject[] a joint designation by a parent and subsidiary." *Id.* Specifically, the preamble to the interim regulations provides that "[f]or purposes of these interim regulations, related companies (e.g., parents and subsidiaries) are considered separate service providers who would file separate Interim Designations." *Id.* (quoting Designation of Agent to Receive Notification of Claimed Infringement, 63 Fed. Reg. 59,233, 59,234 (Nov. 3, 1998)). Based on that language, the court found HFS's argument that it was covered by the designation of its parent company to be "disallowed under the USCO's current scheme for the designation of DMCA agents." *Id.*

Despite its analysis of the interim regulations, the court recognized that the issue of "the validity of a joint DMCA agent designation [was] not squarely presented" because "there was insufficient information in the Hollywood designation to cover HFS in any event." *Id.* at *5 n.7. For that reason, the court declined to expressly decide "whether the USCO's present interpretation of the statute deserve[d] deference or [wa]s otherwise the correct reading of § 512(c)(2)." *Id.* The court's reasoning however, indicates that if presented with the issue, a court could find that a single DMCA agent designation covering multiple entities does not qualify the entities for protection under § 512(c)(2)'s safe harbor.

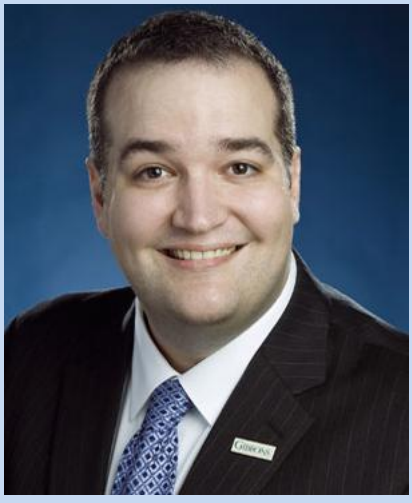
3. A DMCA agent designation on a website alone, without registration with the USCO, is insufficient for a service provider to qualify for safe harbor under § 512(c).

HFS also argued that it was entitled to safe harbor protection earlier than its 2013 registration date because, prior to that time, information concerning a DMCA agent was available on its websites. HFS contended that because it included the proper information on its websites, Plaintiff National Photo Group ("NPG") was able to submit copyright infringement notices to HFS and HFS was able to remedy the alleged infringement by removing the images from its websites.

The court rejected HFS's argument, concluding that even if its factual assertions were true, they were irrelevant. The court explained that "the statutory scheme expressly requires two publicly available, parallel sources of a service provider's DMCA agent information (the service provider's website and the USCO directory) in order for that provider to be shielded by the § 512(c) safe harbor." *Hollywood Fan Sites*, 2015 WL 3971750, at *6. The court found that even if agent information was provided on HFS websites and HFS removed images in response to notices it received from NPG, those actions were insufficient to qualify HFS for the § 512(c) safe harbor because the USCO registration requirement is an express condition under the statute.

C. Conclusion

At least three takeaways result from the *Hollywood Fan Sites* decision. First, because the section 512(c) safe harbor is effective only if there has been a proper DMCA agent designation, service providers should not expect to be shielded from liability for acts of copyright infringement that occur prior to the date of designation. Second, a separate agent designation should be filed for each entity within an organization because, although not expressly deciding the issue, the court in *Hollywood Fan Sites* suggested that a designation covering multiple entities may not qualify the entities for the section 512(c) safe harbor. Third, publication of DMCA agent information on a corporate website alone will not suffice for safe harbor protection; rather, the section 512(c) safe harbor provision requires that the agent information be made available online *and* by publication with the USCO.



J. Brugh Lower, an associate at Gibbons P.C., litigates copyright infringement cases in the Southern and Eastern Districts of New York and the District of New Jersey.

Brugh's practice is focused on counseling and representing clients in a broad range of commercial disputes, with an emphasis on intellectual property. In addition to copyright, Brugh's experience includes trademark, breach of contract, business tort, antitrust, and securities matters.

Prior to joining Gibbons, Brugh served as a law clerk to Chief District Judge Garrett E. Brown, Jr. and Senior District Judge Harold A. Ackerman of the United States District Court for the District of New Jersey and also as a law clerk to the Honorable Helen E. Hoens, Associate Justice of the Supreme Court of New Jersey.

Thinking Ahead to Litigation While Developing Cybersecurity Plans

By Jason E. Glass, Esq.

Even with well-designed policies and procedures, adequate investment in technology, and appropriate management oversight, malicious actors can penetrate an organization's computer network and systems. When a breach incident does occur, an organization can find itself pursuing and/or defending civil lawsuits or responding to regulatory inquires. To effectively prosecute and defend claims arising out of a cyber-event, an organization will need to present a clear and compelling narrative, about its cybersecurity efforts, computer network and systems, and about the breach incident itself. This narrative should include written policies, cybersecurity-related analyses, access and device logs, internal communications, employee declarations, and expert testimony tending to show the organization took appropriate steps to prevent network breaches. An organization also should consider the role of counsel during a breach incident, as well as the costs of litigating cyber-related claims, which may include technical experts, outside counsel, and settlement costs, and whether to insure against such costs.

Documentation

A properly executed cybersecurity effort should be well documented and should include written threat analyses, a tailored set of policies and procedures, and compliance documentation. An organization should consider how this documentation will be viewed by adversaries, regulators, and fact finders. The organization's threat analysis should include adequate consideration of the range of possible threats to the organization's computer systems and network. All reasonably probable attack vectors and corresponding mitigation strategies should be identified; however, an organization need not invest effort in cataloguing truly remote threats. For instance, an organization should address threats to servers and workstations from viruses and spyware, while investing few, if any, resources identifying potential vulnerabilities in a sparsely deployed application lacking access to sensitive data. The threat analysis will inform the organization's overarching cybersecurity policy, which should strive to be clearly written, brief, and non-technical. This ensures that the organization's policy is easily followed within the organization, and readily understandable to anyone outside the organization.

Rather than employ a single policy covering every aspect of the organization's cybersecurity program, an organization should create a suite of policies with varying degrees of granularity, for instance, a high-level program policy (*e.g.*, an organization-wide cybersecurity policy for employees); functional or issue-specific policies (*e.g.*, Internet and e-mail usage policy); and system-specific policies (*e.g.*, intrusion detection systems policy). Whereas organizational policies will be more general, and should be written to last a period of years, issue-specific or system-specific policies can be more detailed, include technical information, and should be updated annually, or as dictated by technological change.

Written policies, however, will not provide sufficient protection in litigation or in regulatory inquires unless an organization can demonstrate that its employees understood and followed them. Consequently, an organization should maintain compliance documentation that maps back to the organization's stated policies and procedures, and demonstrates that these policies and procedures were properly developed, overseen,

and implemented. In addition to the points raised above, the following questions are among those that opposing counsel or regulators might seek to answer following a cyber-incursion, and should in turn drive an organization's thinking about the type and specificity of compliance documentation that should be created and maintained:

- Do the minutes of board of directors meetings reflect director-level consideration and oversight of the organization's cybersecurity?
- Do the organization's policies and procedures adequately address the scope and regulatory requirements of the organization's information technology environment and data collection activities?
- Do the organization's threat analyses, policies, and procedures reflect annual review and updating?
- Does the organization have records of employee attendance at cybersecurity training sessions, as well as employee receipt of cybersecurity policies and procedures?
- Does the organization maintain an accurate network map and inventory of all hardware and software on its network?
- Does the organization's compliance documentation reflect the appropriate management-level authorization for changes to the network or employee access to sensitive data?
- Has the organization maintained access and device logs in order to facilitate the forensic analysis of network and systems activity?

Organizations should also consider how incident response personnel communicate during a crisis situation. E-mail use may be inadvisable during a suspected breach incident, as the malicious actor may have compromised the e-mail server, which will not only render e-mail exposed to unauthorized review, but will also provide the hacker with a window into the breach response, including information that can be used to evade detection. To the extent e-mail is used by incident response personnel, e-mail related to a breach incident is likely discoverable by adversaries and regulators. The mere inclusion of counsel on the distribution list is likely insufficient to support withholding an e-mail as privileged. Therefore, incident response personnel should be discouraged from speculating about the means of incursion, potential vulnerabilities or affected systems, the duration of an incursion, and whether data was misappropriated, among similar topics. These issues should be addressed by a thorough root cause analysis drafted by, or in consultation with, outside counsel.

Evidentiary Considerations

An organization should understand that gathering evidence from computer networks and systems requires skill and training. The organization should train employees so that valuable evidence is not lost or contaminated before a forensic specialist can be engaged. For instance, simply turning off a computer will erase volatile memory. Incident response procedures should provide clear guidance for dealing with potentially infected computers so that the organization can isolate infected systems while preserving evidence. In addition, computers may need to be taken out of service, so the organization should be prepared to substitute properly configured hardware.

Logs from computers, databases, and network devices, such as routers and intrusion detections systems, are instrumental in understanding activity on an organization's computer network and systems. An organization should consider how to lay a proper foundation for getting access and device logs into evidence, including establishing the authenticity and reliability of the logs, *see* Fed. R. Evid. 901, as well as overcoming any hearsay objections, *see* Fed. R. Evid. 803(6) (permitting a party to introduce business records that were produced in the ordinary course of business). Well before a breach incident, the individual most knowledgeable regarding the record-keeping procedures of the organization should be identified so that the

organization can speak authoritatively to counsel, adversaries, regulators, and the court about its computer network and systems.

Direct Legal Involvement

In order to put the organization in the best legal position possible, organizational policies should require in-house counsel participation on incident response teams in circumstances when there is any reason to suspect that sensitive databases, servers, or computers may have been compromised. An organization's breach incident policy should require outside counsel involvement when a breach of a sensitive system has been identified, whether or not the organization knows if data has been misappropriated; once outside forensics expertise is deemed necessary; or circumstances in which law enforcement, a vendor, or a client alerts the organization to a breach incident. Thereafter, outside counsel should quarterback the organization's response through its resolution. Of course, incident response personnel will not know the nature of a breach incident initially, so incident response procedures will have to make clear the triggering events that necessitate escalating the response up the organizational ladder.

Cyber Insurance

The costs of a cyber-incursion can quickly escalate, particularly when sensitive client or organizational data has been misappropriated. An organization likely will need to retain technical forensics experts and outside counsel, and may also engage a public relations firm. In addition, an organization may choose to provide clients whose personal data was stolen with credit monitoring services for a year or more. Typical general liability insurance policies do not cover these costs, and to the extent that such costs may have been deemed to be covered in the past, insurers are adding language that now expressly excludes coverage. Based on a review of its current insurance policies, an organization may need one or more layers of cyber insurance coverage.

Conclusions

Every computer network and system is vulnerable to attack, notwithstanding careful management oversight, strict adherence to a robust set of policies and procedures, and ample human and technological resources. Consequently, every organization should prepare for the eventuality of a cyber-incursion, including contemplating how to best advance its claims and defenses in any subsequent civil litigation or regulatory proceeding. An organization may find it useful to examine its cybersecurity regime from the perspective of a litigation adversary, identifying hard to defend gaps in threat analyses, mitigation efforts, and documentation practices; poorly drafted policies and procedures; or the lack of enforcement of stated policies and procedures. Well before an incursion is detected, an organization should also consider how to collect and preserve evidence in a form that will be admissible in a legal proceeding. Lastly, because the resolution of any cyber-incursion may be costly, an organization may find it advantageous to obtain cyber-insurance coverage to defray some of these expenses.

Jason E. Glass (jglass@wmd-law.com) is an Associate with Wollmuth Maher & Deutsch LLP, where he concentrates his practice on complex commercial litigation, as well as information security and data privacy issues. He has written extensively on cybersecurity, and has been quoted by Compliance Reporter, the Global Association of Risk Professionals, and Financial Planning on cybersecurity issues. He is an (ISC)2 accredited Certified Information Systems Security Professional (CISSP).

Jason has assisted in the defense of financial institutions in federal and state court actions involving mortgage-backed securities, asset-backed securities, and derivatives. His experience spans all phases of litigation, from the complaint through trial. Jason has also been actively involved in representing major Wall Street firms in DOJ, SEC, and state Attorneys General investigations focused on structured products, credit ratings, and insider trading. He has also conducted internal investigations and reviews on behalf of financial institutions.

Jason earned the Chartered Financial Analyst (CFA) designation in 2005 and is a member of the CFA Institute.

The Second Circuit Expands Liability for Retaliation Under The Fair Labor Standards Act

By Saranicole A. Duaban Esq.

For more than twenty years, the Second Circuit has read section 215(a)(3) of the Fair Labor Standards Act ("FLSA") to mean that an employee has a retaliation claim only when he or she formally files a complaint with a government agency for a violation of FLSA, and the employer discharges or retaliates against the employee. *See Lambert v. Genesee Hosp*., 10 F.3d 46 (2d Cir. 1993), *overruled by Greathouse v. JHS Security Inc*., 784 F.3d 105 (2d Cir. 2015). Section 215(a)(3), FLSA's anti-retaliation provision, states that it is unlawful "to discharge or in any other manner discriminate against any employee because such employee has filed any complaint…related to" FLSA's provisions. 29 U.S.C. § 215(a)(3). After a lengthy litigation process, the Second Circuit, in *Greathouse v. JHS Security Inc.*, joined all other circuits to have addressed the issue in holding that FLSA's anti-retaliation provision can be violated when an employee makes an oral complaint to an employer related to violations of FLSA. *See Greathouse*, 784 F.3d at 117.

In *Greathouse*, an employee security guard for JHS Security Inc. complained to the company's president and partial owner, that he had not been paid in several months. In response, the president and partial owner told the employee that he would pay him when he "fe[lt] like it" and drew a gun on the employee. *Id.* at 108. The employee interpreted this act as terminating his employment and filed suit in the Southern District of New York ("SDNY") alleging violations of FLSA, the New York Labor Law ("NYLL"), and retaliatory termination in violation of FLSA § 215(a)(3) and NYLL § 215. *Id.* After neither defendant named in the suit appeared or filed an answer, a default judgment was entered against them. *Id*. The district court referred the case to Magistrate Judge Gorenstein to determine damages. *Id.* Judge Gorenstein determined that the Second Circuit's precedent in *Lambert v. Genesee Hospital* barred recovery for retaliatory termination because the employee did not file a formal complaint with a government agency or other prosecutorial authority. *Id*. Judge Engelmayer adopted Magistrate Judge Gorenstein's report and recommendation except for findings related to liquidated damages and the number of workweeks for which Greathouse had not been paid. *Greathouse v. JHS Security Inc.*, No. 11-7845, 2012 WL 5185591, at *1 (S.D.N.Y. Oct. 19, 2012).

On appeal, Greathouse urged the Court to overrule *Lambert* in light of the 2011 Supreme Court decision in *Kasten v. Saint-Gobain Performance Plastics Corp.*, 131 S. Ct. 1325 (2011) and hold that oral complaints to an employer about perceived violations of FLSA were protected under § 215(a)(3). *Greathouse*, 784 F.3d at 109. The standard in the Second Circuit set by *Lambert* was that in order for there to be a violation of section 215(a)(3), an employee had to file a formal complaint for a violation of FLSA by instituting a proceeding with a government agency or testifying. *Lambert*, 10 F.3d at 55. Specifically, complaints to employers and/or supervisors were not covered by FLSA. *Id.*

Supreme Court's Decision in *Kasten v. Saint-Gobain*

In *Kasten v. Saint-Gobain*, the Supreme Court examined whether § 215(a)(3) can apply to both oral as well as written complaints. *Kasten*, 131 S. Ct. at 1329. The employee in *Kasten* had complained repeatedly to his shift supervisor, human resources, and managers that the location of the time clocks prevented employees from receiving credit for the time it took them to put their work-protective gear on and off. *Id*.

Specifically, the employee followed the company's internal grievance procedure, which called for reporting violations of law to supervisors immediately, then to human resources, and even the human resources at the regional level, if necessary. *Id.* at 1329-30. After making these oral complaints, the employee was terminated for allegedly failing to record his clock-ins and outs on the time clock. *Id.* at 1330.

In evaluating whether the employee's oral complaints could satisfy the statutory term "filed any complaint," the Supreme Court looked to the text, the objectives of the FLSA, and the interpretation espoused by agencies enforcing these provisions. The Court focused on the definition of the word "filed." *id.* at 1331, and found that the term had different meanings depending on the context, but was sometimes used to refer to oral complaints. *Id.* at 1332. Specifically, in regulations and judicial contexts, the term "filed" is used for oral complaints. However, the court acknowledged that other usages of the word "filed" in FLSA refer to a writing. *Id.* The Supreme Court also analyzed the intentions of the drafters of FLSA. *Id.* at 1333. The Court stated that Congress intended for FLSA enforcement to be conducted by employees and not the government. *Id.* Moreover, the Court did not believe that Congress intended to limit enforcement to written complaints when the majority of the workers FLSA was seeking to protect at the time of its passage were illiterate. *Id.* Lastly, the court gave significant weight to the interpretations of the Department of Labor ("DOL") and Equal Employment Opportunity Commission ("EEOC"), the agencies tasked with administering the FLSA. *Id.* at 1335. The Court found particularly compelling that for years both agencies consistently held the view that filing a complaint encompassed both oral and written complaints. *Id*.

The Second Circuit's Decision in *Greathouse v. JHS Security Inc.*

Though the facts of *Kasten* involved an employee complaining to a supervisor, it is important to note that the Supreme Court did not address the question of whether complaints to an employer are covered by section 215(a)(3). In fact *Kasten* goes so far as to explicitly state that that question was not determined by the Court. *Kasten*, 131 S. Ct. at 1334. Therefore, the main issue addressed in *Greathouse* was whether the holding in *Kasten* required § 215(a)(3) to be extended to cover oral complaints to employers specifically.

In *Greathouse*, the Second Circuit utilized the same structural analysis that the Supreme Court employed in *Kasten*. The Court looked at the meaning of "filed any complaint," the purpose of the FLSA, and the interpretation of FLSA espoused by agencies tasked with administering the FLSA. *Greathouse*, 784 F.3d at 112-14. The Second Circuit adopted much of the *Kasten* court's rationale to conclude that there are many interpretations of the word "filed" including oral filings. *Id.* at 112. The Court even acknowledged Scalia's dissent in *Kasten* that all uses of the word "complaint" in FLSA referred to a government filing. *Id.* Nevertheless, the Court ultimately reasoned that a "filed complaint" could also occur in an employer setting when referring to grievance procedures in the workplace. *Id.* at 113.

The Court noted that FLSA's purpose was to "'correct and as rapidly as practicable [] eliminate' labor conditions 'detrimental to the maintenance of the minimum standard of living necessary for health, efficiency, and general well-being of workers[.]'" *Id.*, quoting 29 U.S.C. § 202. FLSA's enforcement scheme also relied heavily on employee complaints. Thus, the Second Circuit found that expanding the retaliation provision to cover complaints to employers would mean faster compliance by employers by protecting employees who come forward before instituting a legal proceeding. *Greathouse*, 784 F.3d at 113-14.

Finally, the Second Circuit gave weight to agency interpretations of FLSA. Like the Supreme Court in *Kasten*, the Court found persuasive the fact that the EEOC and DOL, the agencies that enforce the statute, had for a long time interpreted FLSA's retaliation protection to apply to oral complaints to an employer. Therefore, for all the reasons the *Kasten* court found § 215(a)(3) to apply to oral complaints, the Second Circuit found that § 215(a)(3) applies to oral complaints made to an employer. *Greathouse*, 784 F.3d at 115.

Implications for Practice

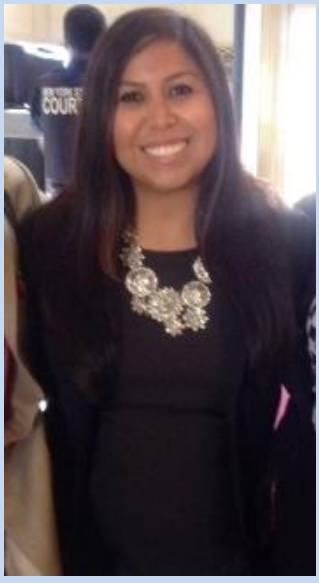
The holding in *Greathouse* certainly brings the Second Circuit in line with the standards employed in other circuits and reflects the realities of interactions between employees and employers in the workplace. However, it also has important implications that both plaintiff and defense attorneys should note.

Because the *Greathouse* court declined to address whether the facts in the case were adequate to state a FLSA retaliation claim, there are some questions left open by the case. The first is to whom must a complaint be made? In *Greathouse* the complaint was made to the president/owner. *Greathouse*, 784 F.3d at 108. Must the employee complain to a supervisor or to someone with the ability to hire or fire? The *Greathouse* court stated that the employer must be on notice that an employee made a complaint, but it is unclear to whom a complaint must be made to in order to put the employer "on notice." Another issue unanswered by the decision is what kind of actions will be considered retaliatory under § 215(a)(3). In *Greathouse*, the employee assumed that having a gun pulled on him was an effective termination. *Greathouse*, 784 F.3d at 108. Employment attorneys can probably safely assume that retaliatory actions would have to be some sort of "adverse action" affecting the terms and conditions of employment, as with retaliation provisions in other statutes. However, *Greathouse* did not squarely answer this question.

The most difficult issue for attorneys to grapple with on both sides may be what suffices as a "filed oral complaint." The Second Circuit adopted the standard set forth in *Kasten*, i.e., that a complaint is orally filed only when that complaint is "sufficiently clear and detailed [that] a reasonable employer [would] understand it, in light of both content and context, as an assertion of rights protected by the statute and a call for their protection." *Id.* at 116 (citations omitted). Employees do not have to state that they have asserted their right under FLSA by name, but it must be more than a mere passing comment. *Id.* What makes this standard even harder to apply is that the Second Circuit specifically declined to address whether the complaint in *Greathouse* would be sufficient under this standard to constitute an orally filed complaint. *Id.*

There has been very little case law in the district courts since *Greathouse* to provide any sort of guidance to practitioners with respect to how the standard will be interpreted. To date, there has only been one notable case addressing the *Greathouse* standard. In *Trowbridge v. Wernicki*, the court vacated a previous dismissal of an employee's FLSA retaliation claims in light of the *Greathouse* decision. *See Trowbridge v. Wernicki*, No. 13-cv-01797, 2015 WL 3746346, at *1 (D. Conn. June 15, 2015). However, *Trowbridge* provides very little guidance because the employee in that case made several verbal complaints as well as written internal communications where he specifically asked about the employer's obligations under FLSA. *Id*. at *5.

In light of these developments, defense counsel and general counsel should modify workplace policies and procedures to ensure that there are adequate grievance or complaint procedures. Further, all supervisory staff, even low-level managers, should be properly trained on how to deal with any sort of complaint, including oral complaints, from an employee. Plaintiff's attorneys should thoroughly question potential clients as to whether any grievance or complaint procedures existed and if the potential client took advantage of them. Plaintiff's attorneys should try to pin down when the oral complaint was made, to whom and whether the employer was placed on notice that the employee was invoking his/her FLSA rights. On both sides, FLSA retaliation claims will become very fact-specific, making litigation of retaliation claims under FLSA more akin to discrimination cases and not as record-based as other wage and hour litigation.



Saranicole Duaban is an employment law associate at Stoll, Glickman and Bellina, LLP. She represents employees in wage and hour individual cases and class actions, employment discrimination cases, and severance negotiations. Prior to joining the firm, she was a fellow at MFY Legal Services in the Workplace Justice Practice where she managed a heavy caseload of wage and hour, employment discrimination, and re-entry cases.

She attended the George Washington University Law School, where she was a member of the Moot Court Board and a Thurgood Marshall Scholar. At GW Law, her passion for advocating for workers was ignited when she worked at the Public Justice Advocacy clinic representing low-income workers in unpaid wage cases at the D.C. Superior Court and in their unemployment hearings.

Saranicole is admitted to practice in the Southern District of New York, the Eastern District of New York, and the State of New York. She is a member of the New York City Bar, the Federal Bar Association Labor and Employment Section, and the National Employment Lawyers Association New York Chapter.

Mark Your Calendar!

October 6, 2015: ***Swearing In Ceremony of SDNY Leadership***

October 20, 2015: ***Securities Law and AML Conference and CLE***

November 16, 2015: ***Asylum Law Conference***

November 19, 2015: ***Women in Law Committee Event – Career Paths for Women Attorneys***

Fall 2015 (Date TBD): ***Meet the Marshal Program***

January 21, 2016: ***Rule of Law Event***