Paragon Risk Management Services Ltd

Paragon Services Newsletter

September / October 2011 ISSUE | 06

Introduction

Paragon Risk Management Services is pleased to introduce you to one of our new Service Providers 'Brandwatch'. As one of the world's leading tools for monitoring and analyzing social media, Brandwatch is the comprehensive and powerful solution needed to make sense of what is being said about brands online.

We know and understand that reputation is paramount to a law firm's continued success and to further demonstrate how Brandwatch can assist from a risk management perspective we invite you to read the following article titled 'Mitigating Online Negativity'.

Furthermore we have included an update from Paragon on the current market for Lawyers Professional Liability and an article from Hinshaw & Culbertson LLP, titled 'Managing Risk when Employees Communicate with Counsel using Employer-Provided E-mail Addresses or Hardware' which addresses some very topical issues.

We hope our Newsletter is of interest to you and would welcome any feedback for future editions.

Inside this issue:

Mitigating Online Negativity

Online Reputation Management

By Dominick Soar at Brandwatch

Over the last year we've seen story after story breaking first on Twitter before reaching traditional media, demonstrating the increasing power of social media in today's communications. For all the benefits of such high-speed information transfer, when it comes to companies and brands trying to manage their reputation, the unprecedented rate at which negative publicity can spread across the web presents a very real hazard.

Whilst online reputation management can and should involve aspects which focus on developing a positive image through techniques like community building and responsive customer service, we will focus here on the reactive kind which is called upon in the case of a major outburst of negativity such as that of a typical PR "crisis".

With a commonly referenced UK case study about Aviva (the sixth largest insurance company in the world by net premium income) from Somatica Digital, we will see how a negative issue can easily spiral out of control online without the presence of a sharp and agile social media monitoring process, causing substantial and ultimately unnecessary damage to a brand.

Case Study

The root of the incident Aviva faced came from a very basic but unresolved customer service issue. Allowing something that a company should be in total control of like this to accelerate so damagingly is a real oversight on Aviva's behalf, particularly when so much worse can happen to a brand and be a lot harder to control.

Background:
In order to change the direct debit details on his insurance policy, Aviva customer Karl Harvard attempted to contact Aviva's customer service team via telephone. After being unable to resolve the issue, he tried a second channel – their online customer portal. When he was met with further problems through this method, Harvard called customer services again in a third and final attempt to sort the issue. Despite making further progress than before, when the line inadvertently went dead it remained unclear as to whether the change had been successfully made.

After this series of poor customer service experiences, Harvard decided to write a letter to the head of Aviva UK, explicating in very thorough detail what had happened. At this point the issue was still contained to Harvard's own knowledge, but shortly after sending the letter he decided to take it online.

Amplification:
Harvard's first move was to publish a summary on his personal blog, embedding a copy of the letter via Slideshare. As the blog had fairly low traffic, Harvard began to seed a link to the Slideshare copy of the letter on relevant consumer complaint communities and conversation around the subject began. Twitter was used to further amplify the conversation and the letter soon made it into Slideshare's most popular documents for that week as well as the news section of customer service community Plebble.

Eventually, on 23rd July, Aviva had become aware of the situation and posted a link to the article on their intranet. At this point, traffic to the blog soared as Aviva's awareness went global. Harvard had been responded to but still no resolution had been reached.

Lasting Impact:
The coverage the letter had achieved on the social web gave it substantial weighting in search engine rankings and ironically the spike in traffic to the blog that was caused by Aviva's internal link to it only gave the site more authority.

The lasting result is that, two years down the line, the blog post still ranks fourth for 'Aviva customer service', along with a thread about it from a personal finance forum at number five.

Could the damage have been limited?
While it's not known how the situation first became known to Aviva, from the spike in traffic it is apparent that it took five days for them to pick up on it. By this point, conversation had already begun to grow and the situation was hard to control.

As proven by this case study, five days was too late in 2009. Now, due to increased adoption of Twitter and heavier general use of social media, the speed at which information spreads has accelerated yet further meaning acknowledgment and response-rates to these kinds of issues need to be a matter of minutes or hours, not days.

Had Aviva realized more quickly that this particular customer issue had been published online, they could have recognized the damage it could cause, consequently upgrading its priority status internally and also been seen to respond directly on the blog, showing their awareness and concern for their customers' satisfaction.

Monitoring and Alerts
Brandwatch and other enterprise-level social media monitoring tools are developed to give brands like Aviva maximum visibility on social media. They have the speed, breadth of coverage and workflow features to ensure a company is fully on top of all conversations taking place about them publicly online whether it's on blogs, forums, news sites, Twitter, Facebook or other social media sources.

By setting up queries for their brands and sub-brands, companies can log in and check their online mentions as frequently as they deem necessary to keep abreast of the most recent conversations about them. The results can then be tagged and categorized as required – they can be assigned to certain members of staff to deal with, flagged if high-priority and deleted if deemed extraneous.

For specific reputation management activities, better still is for alerts to be set up. Brandwatch offers fully customizable and shareable email alerts which can be filtered as required and sent

to any number of recipients at periods of their choice be it daily, hourly or 'as-it-happens'.

This way PR teams, customer service representatives or whoever else might be in charge of online publicity can carry on with other tasks knowing they will be alerted when something happens that might require their attention.

Attitudes and Appropriate Responses

Being fully informed and up-to-date with mentions of a brand online is one thing, but determining what should be done about them, whether they should be responded to and how is a whole different challenge. There are no set rules for this and the approach will often depend on the company's guidelines for external communication. One common basic principle that applies to most situations is to avoid getting into discussions in a public domain and to try and direct the issue offline so that it can be handled privately without causing more damage.

One thing to also note is that in social media in particular, transparency and personal touches are much appreciated and can win brands favor far more successfully than hiding behind corporate shields. Along with the potential hazards of corporate interaction on social media, this is one of the reasons more and more companies are developing official internal social media policies.

So of course, there are reputation management issues that extend far beyond the realms of social media monitoring; procuring a robust and sophisticated monitoring tool cannot account for or direct companies' attitudes towards crisis management. Companies that, as The Economist put it for example, fall guilty of "the three cardinal sins of PR: becoming the story; getting caught; and appearing to attempt a cover-up" must look more deeply at the way they handle PR problems.

However, as well as assessing fundamental attitudes to crisis management and PR problems, it is becoming increasingly important for companies to stay up-to-date with what is happening surrounding their brand online and that is an essential element of reputation management that social media monitoring can assist in.

www.brandwatch.com

Paragon Market Overview

State of the Market for Lawyers Professional Liability in 2011

By Nick Lewin, Director and Partner of Paragon International Insurance Brokers Ltd

There is no doubt that across the board those insurers writing large Firm Lawyers Professional Liability have seen their profit margins eroded over the last four years to the extent it is doubtful whether they are any longer making money from this class.

Rates have steadily come down on a year by year basis, investment income has plummeted and claims inflation has continued to rise. There are currently some significant nine figure claims in the market which insurers will likely pay.

Does this mean we are about to enter a hard market? Not necessarily.

Many insurers have over the last three years recorded record headline profits at a time when nearly everyone else is suffering from the worst economic crisis for over 60 years

Insurance has become somewhat of a safe haven for investors, which has resulted in a substantial increase in capital in the market leading to both new start up insurers and many established insurers trying to expand their base.

To date we doubt very much if the headline catastrophes of 2011 will be anything more than an earnings event. Earnings events do not traditionally change markets.

Indeed we would not be surprised to see a continuing expansion in the Capital base in 2012 at a time when the western economies may well be either in or close to recession. Supply may outstrip demand leading to further competition.

While there may not be much room for any significant further softening we will continue to argue that insurers should be seen to adjust their lofty expectations downwards, cut their cloths to meet the current environment, judge each client on its merits and not unfairly seek to penalise clients that continue to show profitable claims records for insurers.

Managing Risk When Employees Communicate With Counsel Using Employer-Provided E-mail Addresses or Hardware

By Anthony E. Davis and Katie M. Lachter[1]

It has become routine for employees to send personal e-mails from the workplace, either using their employer-provided e-mail account or through a Web-based e-mail provider such as Yahoo! or Google but using employer provided hardware – whether PDA's or computers. E-mail communications necessarily exist in multiple environments simultaneously. Copies of e-mails reside in multiple locations (servers, PDA's, laptop and desktop hard drives, and backup media), and are accessible to anyone with access to those systems even after the sender has left the company. As a result, communications that employees intend or believe to be personal and confidential may (and probably will) wind up being examined by their employer, or possibly even third parties – perhaps unbeknownst to and/or against the wishes of the employee. But the consequences can be more critical than mere discomfiture for the employee. If an employee communicates with his personal attorney via his work e-mail account or computer, he risks losing the protections of the attorney-client privilege that would otherwise be afforded to such communication. This article explores the circumstances that may give rise to this loss of the privilege and the duties that lawyers and law firms may owe to clients to warn of and advise with respect to this risk.

Development of Case Law

In recent years a body of case law has developed addressing situations in which employees seek to assert privilege over e-mail communication with attorneys, and their employers (or others) argue that the privilege has been waived.

Asia Global

In 2005, the United States Bankruptcy Court for the Southern District of New York established a framework for deciding such cases in In re Asia Global Crossing, Ltd., 322 B.R. 247 ("Asia Global"). In that case, former employees of the debtor corporation used the corporation's e-mail system to communicate with their personal attorney concerning actual or potential disputes with the corporation. The court first noted the prevailing view that "lawyers and clients may communicate confidential information through unencrypted e-mail with a reasonable expectation of confidentiality and privacy" (citing several ethics opinions, although these opinions did not address employer-provided email accounts or hardware). Put another way, a communication that would otherwise be protected by the attorney-client privilege does not lose that protection merely by virtue of having been sent by e-mail. Consistent with this trend, New York and California have enacted laws to this effect. See N.Y. C.P.L.R. § 4548 (McKinney 1999); Cal. Evid. Code § 917(b) (West 2004).

Next, recognizing the lack of prior decisions discussing the confidentiality of an employee's e-mails in terms of the attorney-client privilege, the court looked to cases addressing the analogous question of the employee's expectation of privacy in his office computer and the company e-mail system. A right of privacy is recognized under both the common law (the tort of "intrusion on seclusion") and the Fourth Amendment to the United States Constitution. In both cases, the aggrieved party must show a reasonable expectation of privacy. The court further noted that, as with attorney-client confidentiality, the expectation of privacy has both subjective and objective components, i.e., the person asserting the right must show a subjective expectation of privacy that society accepts as objectively reasonable. Finally, the court analogized an employee's expectation of privacy in communications sent from his work e-mail account or computer to his expectation of privacy in his office, desk, and files, relying on O'Connor v. Ortega, 480 U.S. 709 (1987).

In O'Connor, a physician employed by a state hospital challenged the hospital's use of materials seized from his office in administrative proceedings resulting in his discharge. While he was on administrative leave, hospital officials, ostensibly in order to inventory property, searched his office and seized personal items from his desk and file cabinets. In determining that the employee had a reasonable expectation of privacy in his office, the Supreme Court recognized longstanding societal expectations of privacy in one's workplace, noting that "it has long been settled that one has standing to object to a search of his office, as well as of his home …." Id. at 716. Some employees' expectations of privacy "may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." Id. at 717. Given the wide variety of work environments, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.

---

[1] Anthony E. Davis is a partner, and Katie M. Lachter an associate, in the Lawyers for the Profession® practice group of Hinshaw & Culbertson LLP. Both are based in the firm's New York office.

Based on its survey of workplace privacy cases, the Asia Global court enumerated four factors that should be considered in determining whether an employee had a reasonable expectation of privacy in his workplace e-mail communications, in order to avoid being found to have waived the attorney client privilege: (1) whether the corporation maintained a policy banning personal or other objectionable use; (2) whether the company monitored the use of the employee's computer or e-mail; (3) whether third parties had a right of access to the computer or e-mails; and (4) whether the corporation notified the employee, or the employee was otherwise aware, of the company's use and monitoring policies. On the facts before it, the court determined that it lacked sufficient information about the corporation's e-mail policies to determine as a matter of law that the use of the company's e-mail system had waived the attorney-client privilege, and ordered further proceedings.

Application of Asia Global

Both state and federal courts across the country have subsequently applied the Asia Global factors to determine when the privilege has been waived, and the divergent outcomes in these cases demonstrate the highly fact-specific nature of the inquiry. In Scott v. Beth Israel Medical Center, 847 N.Y.S.2d 436 (N.Y. Sup. 2007), plaintiff Scott, a doctor, brought a breach of contract action against his former employer, Beth Israel Medical Center, arising from the termination of his employment. After learning from counsel for Beth Israel that it was in possession of e-mail correspondence between plaintiff and his counsel that had been transmitted using Beth Israel's e-mail system, plaintiff moved for a protective order requiring Beth Israel to return all such e-mail correspondence, asserting (among other grounds) attorney-client privilege.

Beth Israel countered that the e-mails were never protected by the attorney-client privilege because plaintiff could not have made the communications in confidence when using Beth Israel's e-mail system, as such use was in violation of Beth Israel's e-mail policy. That policy stated: "[a]ll Medical Center computer systems … electronic mail systems, Internet access systems, … and the wired or wireless networks that connect them are the property of the Medical Center and should be used for business purposes only." Additionally, "[a]ll information and documents created, received, saved or sent on the Medical Center's computer or communications systems are [sic] of the Medical Center. Employees have no personal privacy right in any material created, received, saved or sent using Medical Center communication or computer systems. The Medical Center reserves the right to access and disclose such material at any time without prior notice."

Applying the Asia Global factors to the facts, the court determined that plaintiff either had actual knowledge of the policy, or had constructive knowledge by virtue of his position as an administrator. Consequently, plaintiff's communications with his attorney in violation of Beth Israel's policy were not made in confidence, and plaintiff had therefore waived the attorney-client privilege, if it ever applied. In reaching this result, the court reasoned that the effect of an employer e-mail policy such as that of Beth Israel is akin to having the employer looking over the employee's shoulder each time an e-mail is sent, and therefore, plaintiff's messages could not have been communicated in confidence.

Similarly, in Leor Exploration & Production LLC, et al. v. Aguiar, 2009 WL 3097207, the Southern District of Florida considered whether documents the client transmitted to his counsel by e-mail, using the adverse party's server, thereby lost the attorney-client privilege under Florida law. Citing the Asia Global criteria, and finding that each element had been met, the court concluded that there was no reasonable expectation of privacy regarding communications transmitted through the employer's e-mail server, and therefore held that the privilege had been lost. Specifically, the court noted that the employee handbook states that [employer] owns all electronic communications and that individuals using the [employer] e-mail system have no expectation of privacy. The [employer] employee handbook expressly states: "Employees should have no expectation of privacy with regard to communications made over [employer]'s systems." The employee handbook further advises that "[employer] representatives may access and monitor the use of its systems and equipment from time to time" and that "employees should not use [employer]'s electronic … communications systems to communicate, receive, or store information that they wish to keep personal or private."

Most recently, in Holmes v. Petrovich Development Company, LLC, 2011 WL 117230 (Cal.App. 3 Dist., Jan. 13, 2011), the employee, Holmes, argued that she believed her personal email would nonetheless be private because she utilized a private password to use the company computer and deleted emails after they were sent. She also argued that, because the company did not actually access or audit employees' computers, the "operational reality" was such that she could reasonably expect her email communications were confidential. Consistent with the other cases discussed above, the California Court of Appeal rejected both arguments and held that Holmes' belief that her communications were confidential was unreasonable because she had been adequately warned that the company would monitor email to ensure employees were complying with office policy not to use company computers for personal matters, and she had been told that she had no expectation of privacy in any messages she sent via company computers.

However, in Convertino v. United States Department of Justice, 674 F.Supp.2d 97 (2009), the District of Columbia applied the Asia Global test and reached the opposite conclusion. In that case, plaintiff had filed a complaint against the U.S. Department of Justice ("DOJ") alleging that DOJ had willfully and intentionally disclosed information to a reporter for the Detroit Free Press in violation of the Privacy Act, 5 U.S.C. § 552a. The disclosed information consisted of documents from an investigation into Plaintiff's conduct by DOJ's Office of Professional Responsibility. Plaintiff moved to compel production of 736 documents DOJ had classified as privileged. Included among these documents were emails from an individual employee of DOJ, Jonathan Tukel, who was originally named as a defendant but was dismissed. The DOJ did not assert the privilege, but Tukel intervened to argue that e-mails sent and received by him to and from his personal attorney using his government e-mail address and over the government's server were entitled to be treated as privileged. Tukel had hired an attorney in anticipation of litigation against him by Plaintiff, but the case does not discuss the content of those emails or whether there was any information damaging to Tukel or DOJ.

The court agreed with Tukel that his emails to his attorney were privileged. Noting that "[e]ach case should be given an individualized look to see if the party requesting the protection of the privilege was reasonable in its actions," the court found that "on the facts of this case, Mr. Tukel's expectation of privacy was reasonable. The DOJ maintains a policy that does not ban personal use of the company e-mail. Although the DOJ does have access to personal e-mails sent through this account, Mr. Tukel was unaware that they would be regularly accessing and saving e-mails sent from his account. Because his expectations were reasonable, Mr. Tukel's private e-mails will remain protected by the attorney-client privilege."

The Convertino case is notable in that it is the only published decision to date addressing an employee's invocation of attorney-client privilege in his workplace email where the interests of the employee and employer were not adverse. Unlike the rest of the cases applying the Asia Global factors, here the employer was not seeking to defeat the privilege. Nor did it

affirmatively invoke the privilege, as might happen in a case in which the employer's and employee's interests are aligned. As ethicist Jeremy Feinberg noted in 2008, "Well-established doctrines such as the joint-defense and common-interest privileges might well apply, under appropriate circumstances, if both employer and employee are sued in the same case, are cooperating, or coordinate their legal strategies."[2] As Feinberg also points out, in other contexts, courts have reached inconsistent conclusions when an attorney-client communication is shared with a party who has every reason to want to maintain the privilege, but does not have a common-interest or joint-defense arrangement. In Stroh v. General Motors, 213 A.D.2d 267 (1st Dep't 1995), a New York State appellate court held that a mother, injured in a car accident, could speak with her lawyer in the presence of her daughter (who was not a party to the lawsuit) without destroying the privilege. On the other hand, in the prosecution of Martha Stewart, a federal court held that Ms. Stewart waived attorney-client privilege when she forwarded to her daughter an email written to her attorney. United States v. Martha Stewart, 284 F. Supp. 2d 461, 462 (S.D.N.Y. 2003). In Convertino, even in the absence of a joint-defense or common-interest arrangement, the court held that the privilege was not broken due to the employee's inadvertent disclosure of his emails to his employer by virtue of using his employer-provided email address. Convertino thus stands for the proposition that, with respect to attorney-client privilege and employer email addresses or hardware, the same privacy analysis applies regardless of whether employees and employers are adverse to each other.

These cases, taken together, establish that where an employer clearly, explicitly and unequivocally prohibits personal use of its computers and servers, and advises its employees that it reserves the right to monitor and review their electronic communications, then the employees will have great, and likely insurmountable difficulty claiming that communications sent to their attorneys using the employer's technology are entitled to the protection of the attorney-client privilege because, in these situations, they had no reasonable expectation of privacy.[3]

Personal E-mail Accounts

The cases discussed above deal with the situation where an employee uses his workplace e-mail account to transmit purportedly confidential communications. A variation on that theme is the use of a private e-mail account accessed via the Internet from the workplace. Two cases that have addressed this issue both conclude that the same considerations apply, but with particular emphasis on the wording of the employer's e-mail and Internet usage policy. In Long v. Marubeni America Corp., 2006 U.S. Dist. LEXIS 7659 (S.D.N.Y. Oct. 19, 2006), employees claimed attorney-client privilege with respect to e-mails sent from private, password-protected e-mail accounts on their work computers to their attorneys, concerning litigation that they wished to pursue against their employer. Unbeknownst to the employees, these e-mails were stored on the employer's computers in temporary Internet files, in a separate folder that was accessible to other authorized employees of the company.

The employee handbook explicitly stated that "all communications and information transmitted by, received from, created or stored in [the work computers'] automated systems … are company records" and company property, and that the company had the "right to monitor" its automated systems. It further stated that "employees have no right of personal privacy in any matter stored in, created, received, or sent over the … word processing and/or internet systems provided by the company. Without referencing the Asia Global factors, the court held that in light of the language in the employee handbook, the "confidentiality element" did not exist, and the "assertion of the attorney-client privilege to safeguard" the communications from disclosure was improper. Central to the court's reasoning was the fact that the employees elected to use their work-assigned computers to communicate with their attorney about their employer, and that they knew or should have known about the company's computer use policy.

In a more recent case, Stengart v. Loving Care, 973 A.2d 390 (N.J. Super. July 29, 2009), an employee sent e-mails to her attorney using a company-issued laptop computer through a personal, password-protected Web-based (Yahoo!) e-mail account. The e-mails concerned a lawsuit the plaintiff/employee contemplated bringing against her employer, and were sent to the employee's personal attorney prior to her resignation from the employer. After the [then former] employee sued the company, the employer obtained the e-mails by making a forensic image of the computer's hard drive and extracting them from the plaintiff's Internet browser history.

There was a factual dispute in Stengart over whether the company's electronic communications policy was in effect or was merely in draft form at the time plaintiff sent the e-mails, and whether the policy applied to plaintiff (who was an executive). While the New Jersey appellate court noted that the privilege issue should not have been decided absent an evidentiary hearing, it ultimately concluded that the words in the handbook did not convey a clear and unambiguous warning that the employer might attempt to seize and retain personal e-mails sent through the company's computer via the employee's personal e-mail account. Indeed, the policy explicitly permitted "occasional personal use" of its systems. The court concluded that the e-mails were privileged on public policy grounds, holding that the policy considerations underlying the attorney-client privilege "substantially outweighed" the company's interest in enforcing its computer use and electronic communications policy.

Risk Management Lessons

In light of these cases, lawyers need to consider giving explicit advice at the outset of every representation of individual clients regarding the use of e-mails for communications that the client wishes to have treated as confidential. This advice should make clear that any use of the employer's hardware – not just an e-mail address provided by the employer – may result in waiver of the attorney-client privilege. Similarly, the advice should point out that the risk may not be limited to loss of privilege in disputes with the employer, but may apply to others adverse to the client, on the basis if the privilege is lost in one context because privacy of such email communications cannot be reasonably expected by the employee, it may be lost generally. This can be accomplished, in the first instance, by adding appropriate language explaining and warning of the risks of communications that involve the use of any employer owned or operated technology in all engagement letters issued by the lawyer and the firm to their new clients. However, because the loss of the attorney-client privilege could be such a devastating blow to a client's case, the attorney should, in appropriate circumstances, consider whether to advise the client not to communicate

[2] Jeremy R. Feinberg, "Risky Business: E-mail at Work for Personal Purposes," The New York Professional Responsibility Report, January 2008.

[3] This is true even where the employee argues that the "operational reality" was that the company did not enforce its computer and e-mail monitoring policies. Holmes v. Petrovich Development Company, LLC, 2011 WL 117230 (Cal. App. 3 Dist., Jan. 13, 2011).

with the attorney using an employer-provided email account or employer-provided hardware unless the attorney has examined the employer's policies and procedures regarding the employer's right to access an employee's emails and has given an opinion that the client-employee has a right to expect privacy with respect to such email communications. Absent such an opinion, attorney-client communications for which confidentiality and the privilege are important to preserve should be handled through a medium other than the employer's computer network or hardware. The cost of a personal laptop or other device that can access and send emails, and of a personal, password-protected email account, are small prices to pay for preserving the attorney-client privilege and for protecting the attorney against risks of malpractice.

Conversely, counsel for organizations should consider advising their clients to draft and regularly circulate explicit and comprehensive technology use policies regarding employees' lack of expectation of privacy from any use of company supplied technology – not just the company supplied email address.

One important caveat on the employer side of the issue needs to be noted, both by entities and their counsel. Even where an organization is confident that its policy effectively removes its employees' expectation of privacy, an employer that intercepts potentially privileged or confidential information pursuant to its policy should take care before deciding to read or to use the intercepted material. The client should notify in-house counsel or outside counsel immediately. Counsel, in turn, should also take great care before reading or using such intercepted material, given that such use (and the policy alleged to permit the intended use) may still be susceptible to challenge. At the very least, some form of notice to the employee may be required in order to establish the scope of ethical and legal duties under the circumstances presented. Indeed, in Stengart, the court chastised the employer's outside counsel for "appoint[ing] itself the sole judge of the issue" and making use of the e-mails in question "without giving plaintiff an opportunity to advocate a contrary position." 973 A.2d at 403. Failure to consider the relevant law and rules of professional responsibility before using information obtained from employee e-mails may result in disqualification or sanctions, including a directed adverse outcome in the underlying dispute.

These articles are published without responsibility on the part of the publishers or authors for any loss occasioned by any person acting or refraining from action as a result of any views expressed therein.

Effective risk management advice requires detailed knowledge and analysis of firm and/or practice area specific facts relating to the risk. The information included in this newsletter cannot and does not attempt to satisfy this requirement for any of its readers.

Some Key Conference Dates:

New York
October 20-21, 2011
Hildebrandt Institute - 10th Annual COO and CFO Forum
Balancing Growth and Profitability in Times of Economic Uncertainty

Chicago
February 29 – March 2, 2012
Legal Malpractice and Risk Management Conference

Philadelphia
April 15 – 19, 2012
Risk & Management Society Inc (RIMS) Annual Conference

Paragon Services is dedicated to providing our clients with as many additional resources as possible. Throughout our travels we are meeting with all types of law firms and risk management specialists and we constantly hear about the current risk management issues and 'who' is working with 'who' to resolve these. If we can help you and your firm with any risk management plans, please do not hesitate to contact us.

Robert R. Feagin, III	John Steele	James Kalbassi	Nick Lewin	Natasha Watson
Special Counsel to Paragon Risk Management Services Ltd	Special Counsel to Paragon Risk Management Services Ltd	Director	Director	Director
rfeagin@paragonbrokers.com	john.steele@johnsteelelaw.com	jkalbassi@paragonbrokers.com	nlewin@paragonbrokers.com	nwatson@paragonbrokers.com
(850) 766 0033	(650) 320 7662	(011) (44) 20 7280 8202	(011) (44) 20 7280 8231	(011) (44) 20 7280 8216