

Winter 2011

Hedge Funds: The New Normal

By James S. O'Brien, Marsh FINPRO PEMA Managing Director and Susan F. Friedman, Marsh FINPRO Senior Vice President and Claims Advocate

FBI raids, seizure of documents, search warrants, leaked information, industry-wide probes, criminal behavior, arrests, government investigations, subpoenas, epidemic insider trading, failure to cover losses from bad bets, conspiracy, regulation, and compliance are all among the headlines of media coverage of the hedge fund universe.

Yet, notwithstanding media reports of high profile scandals, hedge funds have made a herculean recovery from the severe downturn in 2008. In 2010, however, hedge funds yielded smaller profits than in 2009 and assets under management stagnated at approximately \$1.9 trillion at the close of third quarter, up only marginally from the \$1.82 trillion managed in early 2010, according to Absolute Return and Marketwire.

Further, Hedge Fund Research Inc. reports that industry liquidations seemingly returned to their pre-liquidity crisis levels. The total number of fund closures for the first half of the year was 417. Though many hedge funds lost money and suffered redemptions during the first two quarters of 2010, the largest firms in the industry increased assets, albeit slightly. In fact, for the first half of 2010, an estimated \$23 billion in new investor capital was allocated to firms with greater than \$5 billion in assets under management, thereby evidencing a clear investor preference for the most well established firms. As expected, these firms control an estimated 60 percent of all hedge fund industry capital.

Despite the rebound of hedge funds, market volatility still exists. Yet

with stable consistent performance, improved structural integrity, and renewed investor confidence, hedge fund managers have been able to surpass their previous highs in the third quarter of 2010 and anticipate a solid finish through year end. The challenge, going forward, will be to find balance between investor demands and the needs of the management company and to remain agile enough to evolve in the face of new regulations.

In today's economy, it is increasingly important that hedge fund managers fully understand the concerns of their investors in order to attract and retain capital and effectively mitigate their exposure to liability. During the past 12 months, investors have focused on hedge fund structures, fees, liquidity terms, redemption restrictions, and compensation. Investors have had an insatiable appetite for transparency and seek greater clarity as to a hedge fund manager's investment philosophy and processes. Additionally, investors' focus extends to independent valuation, scrutiny of prime brokers, auditors, custodians, and legal advisers used by hedge funds. Operational due diligence, expanding monitoring processes, understanding back-office capabilities, providing adequate disclosure, and ensuring investor



Table of Contents

1 Hedge Funds: The New Normal

3 Uninsured Theft and Fraud Losses? What a Crime!

5 Is Anything Really Private Anymore? Regulatory Update from Cyberspace

7 Employment Practices Liability: The Good, the Bad, and the Ugly—A Year in Review

protection via proper hedge fund corporate governance and risk management are all top priorities for investors.

Claims by investors have alleged breaches of fiduciary duties, failure to follow investment guidelines, conflicts of interest, inaccurate or misleading asset valuation/reporting, fraud, inappropriate fees, misappropriation of fund assets, unwarranted restrictions on redemptions, racketeering, misrepresentation in fund marketing materials or other information disseminated to investors, lack of diversification, and failure to perform due diligence on investments, among others. Additionally, outside third party claims from investors of target takeovers have asserted unlawful attempts by co-investors to “claw back” money from investors (who exited defunct funds just before their collapse), share price manipulation, short selling to drive down stock prices, and mismanagement.

Claims against hedge funds have also included derivative actions, straddle-claims following a change in control, lawsuits by bankruptcy trustees, employment litigation, fidelity/criminal conduct, litigation surrounding broken deals/financing issues, legal actions related to acquisitions, lawsuits alleging breaches of fiduciary duty pursuant to the Employee Retirement Income Security Act (ERISA)—a federal law that governs pension and health/welfare insurance plans—and cyber/data security breaches. Additionally, there is an acute awareness by investors of newly-enacted legislation and regulations.

On November 19, 2010, the Securities and Exchange Commission (SEC) proposed new rules and amendments to the Investment Advisers Act of 1940, as mandated by certain provisions of the Dodd-Frank Wall

Street Reform and Consumer Protection Act (Dodd Frank). The Act requires all hedge funds with \$150 million or more in assets under management to:

- register with the SEC;
- disclose the dollar amount of their assets under management, the types of investors in the fund, and all fund auditors, prime brokers, custodians, administrators, and marketers;
- appoint a chief compliance officer;
- establish a code of ethics; and
- comply with custody and record keeping requirements.

Not only are hedge funds confronted with the new challenges brought by registration requirements, but they also face a revitalized SEC. The agency reports a 113 percent increase in the number of formal investigations, an 82 percent jump in the issuance of temporary restraining orders, a 170 percent rise in disgorgement of profits cases, and a 35 percent increase of penalties imposed. Although the SEC typically focuses its investigations and enforcement actions around uncovering fraud and securities law violations, misrepresentations in performance, issues with valuation (including side pockets), faulty disclosure practices, insider trading and related criminal activity, failed compliance, side letters, custody and asset verification, and conflicts of interest, there has been a marked increase in “sweep or theme” (targeting the “issue du jour”) and “cause or surprise” (SEC investigators acting on a “tip” show up unannounced) inspections. Additionally, there seems to be an increased interest in performance and marketing, books and records, and layering/spoofing cases where a firm enters into numerous layered non-bona fide market moving orders to generate interest. The SEC and

investors both find side letters and selective disclosure particularly troublesome, although not illegal.

The “new normal” continues with the passage of Section 922 of Dodd-Frank, the whistleblower bounty provision, which provides that whistleblowers are eligible for additional rewards for reporting alleged securities violations to the SEC—up to 30 percent of funds recovered. Overall, the uncertainty surrounding the implementation of Dodd-Frank is of great concern to hedge funds and their investors, as many commentators opine that it will dramatically alter the current landscape. Certainly, the enhanced authority of the SEC, via Dodd Frank, with an additional 400 employees expected to be hired as part of the 2011 U.S. fiscal budget, will strengthen this formidable regulator. In addition, the combined forces of the SEC with other U.S. regulatory bodies including the Department of Justice, IRS, Commodity Futures Trading Commission, Financial Industry Regulatory Authority (FINRA), and those abroad make for a charged regulatory environment.

The anticipated regulations and their enforcement will likely affect established players and emerging players alike. In order to stay ahead of the curve many hedge funds are ramping up due diligence and compliance efforts as well as purchasing insurance for future protection in the event of a claim.

As hedge funds face a growing number of investigations and legal actions, many now attempt to appeal to insurance underwriters by demonstrating good corporate governance and disclosing information pertaining to SEC registration, their investment strategies, valuations, redemption terms, level of activism, investor profiles, background of principals, amount and types of assets under

management, risky investments, operating and performance history, side letters, legal structure, prime brokers, custodians, auditors, and any other information that could potentially lead to claims activity. Satisfactory and sufficient information enables hedge funds to purchase general partnership

liability, directors and officers liability, professional liability/errors and omissions, cyber/network security, employment practices liability, ERISA/fiduciary liability, and fidelity/crime insurance, or whatever it is determined best meets their needs. #

For more information please contact your FINPRO representative or the authors of this article, James O'Brien at James.Obrien@marsh.com or (212) 345-6432 or Susan F. Friedman at Susan.F.Friedman@marsh.com or (212) 345-6500.

Uninsured Theft and Fraud Losses? What a Crime!



By Kevin Guillet, Marsh FINPRO Fidelity/Fraud Product Leader

Employee dishonesty and other types of fraud cost U.S. businesses billions of dollars each year. Fraud is also a leading cause of business bankruptcies. According to the Association of Certified Fraud Examiners' 2010 Report to the Nations on Occupational Fraud and Abuse:

- organizations typically lose 5 percent of their revenue to fraud;
- the median cost of a fraud event is \$160,000, with nearly one-quarter reaching \$1,000,000 or more;
- the median duration is 18 months before a fraud is detected;
- small organizations disproportionately fall victim to fraud; and
- more than 85 percent of fraudsters have never been previously charged with nor convicted of a fraud.

The Surety & Fidelity Association of America—which tracks crime insurance results of most U.S. insurers—reports that for the period 2005 to 2009 insured losses totaled approximately \$1.6 billion, including almost \$560 million in 2009 alone. The total amount of insured losses in the U.S. is likely higher as these figures do not include insured losses under policies written by non-U.S. insurers, such as those operating out of London or Bermuda.

Crime insurance policies, which are often referred to as fidelity bonds, protect organizations from direct financial loss arising out of dishonest and fraudulent acts committed by their employees as well as specific types of fraudulent or criminal acts committed by non-employees, including theft, burglary, robbery, forgery, fraud, and computer theft.

The Mechanics of Crime Insurance Policies

Crime insurance policies typically require that all insured entities be scheduled on the policy for coverage to apply. If requested, many insurers will endorse the policies to cover all commonly owned or managed entities, eliminating the need to schedule each entity individually. These policies typically cover property—including money and securities—that is owned by the insured. Most policies also cover property of others that is held by the insured in any capacity, as well as property of others for which the insured is legally liable. An example of the latter is property of another that is held by the insured, which the insured then entrusts to a third party.

Crime insurance policies can be written on either a discovery or a loss sustained basis. A policy written on a discovery basis covers loss that is discovered during the policy period regardless of when it occurred. A policy written on a loss sustained

basis covers loss that both occurs and is discovered during the policy period. Notably, a loss sustained prior to the policy period in which it is discovered if coverage has been continuously in force from the time the loss occurred until the time it was discovered.



Unlike a liability policy, when a loss occurs, a crime insurance policy requires that the insured prove that the loss is covered before the policy will respond. This means that the insured must provide a written proof of loss, often within six months of discovery of the loss. If law enforcement is involved or the loss is complex in nature, an insured may need more time to prepare and submit a proof of loss: time extensions are often granted by insurers.

As with any insurance policy, crime insurance policies contain a number of exclusions. Exclusions to coverage commonly cited by insurers include:

- indirect or consequential loss of any nature,
- loss of potential income, and
- loss caused by an employee after the insured has knowledge of prior dishonest acts committed by that employee.

Underwriting to the Crime Exposure

Insurers look favorably upon insureds with the following characteristics:

- Audited financial statements with an unqualified opinion.
- Consistent, stable financial performance over time.
- Positive financial performance relative to peers.
- A robust internal control environment.
- Strong controls over disbursements.
- Independent internal audit function.
- Clean CPA letter to management on internal controls.
- Clean loss history (organizations that have suffered a loss should show clearly defined remedial actions taken to prevent future losses of the same type).

Most insurers focus on the following areas when underwriting crime insurance policies.

- **Audit and control environment.** Is an annual CPA audit performed? Are disbursements subject to dual control? Are bank statements reconciled on a timely basis?
- **Hiring practices.** Are background checks performed on new hires?

- **Management of vendor relationships.** Are background checks performed on new vendors? Are competitive bids required? Is the accounts payable process fully segregated so no one person can control it from beginning to end?
- **Downsizing.** What is the impact on employee moral? How has downsizing impacted staffing of control functions (compliance, internal audit, corporate security, etc.)?
- **Foreign exposures.** Are significant operations located outside the U.S.? Are treasury functions for non-U.S. operations centralized in the U.S. or administered locally?
- **Outsourcing.** Are critical functions outsourced to third parties?

Every organization—large or small, public or private, for profit or non-profit—is exposed to the perils insured under a crime insurance policy. An uninsured crime loss can do irreparable harm to an organization's balance sheet. It may also have a significant negative affect on an organization's reputation if the loss involves property entrusted to it by a customer. The crime insurance marketplace features numerous well-rated insurers catering to the needs of all types of organizations. Further, an abundance of capacity serves to keep premium rates stable. It is for these reasons, among others, that crime insurance should be considered an integral component of any comprehensive insurance program. #

For more information about this topic, please contact your FINPRO representative or the author of this article, Kevin Guillet at Kevin.Guillet@marsh.com, (212) 345-8095.

Is Anything Really Private Anymore? Regulatory Update from Cyberspace



By Robert Parisi, Marsh FINPRO Cyber & Technology Product Leader

An active and increasingly aggressive regulatory climate has evolved in North America around the issues of information security and privacy beginning in 2003, when the first state privacy breach notification law came online. Unlike earlier privacy regulations in Europe, the U.S. regulations concern themselves less with usage than with reaction to fortuitous events—e.g., how to properly store milk versus cleaning up spilled milk.

The U.S. laws fall into three categories.

1. laws imposing duties following a security breach;
2. laws prescribing how information is to be secured or stored; and
3. laws requiring companies to implement and establish crisis management programs.

Generally, the states have led the way in enacting regulations requiring commercial entities to provide notice (i.e., to their customers) in the event that the entity loses or mishandles personal information. Although California was a trail blazer, nearly all U.S. states and territories have

adopted a breach notification law, including Puerto Rico, the U.S. Virgin Islands, and the District of Columbia. Unfortunately, these notification laws can vary dramatically—some require an expansive explanation of the underlying event while others actually restrict what the notice relates about the event. In this regard, the regulations all differ slightly on the triggers that require notice as well as the form that the notice must take. The one thing that all the regulations have in common, though, is that they only concern themselves with the private information of their own citizens. This can be especially problematic for companies that touch citizens of several states as they will be forced to comply with each state's regulation, as opposed to just the regulation of the state they happen to be operating from. On the federal level, while there has been noise, no effective action to harmonize these disparate state breach laws has taken place. It appears unlikely that any such action will occur in the immediate future.

Several laws allow for certain safe harbors, such that notice may be avoided if certain facts can be established, the most common being that the lost data is encrypted.

Unfortunately, these safe harbors do not overcome the language in several of the notification statutes that trigger a duty to notify persons/customers if the entity knows or believes that personally identifiable information may have been disclosed or mishandled.

Another seemingly mitigating clause in several states' laws is the catastrophic breach provision. This provision allows an entity to utilize media avenues, other than direct mail, to notify the "victims" if the pool of "victims" is large enough and/or the cost of individual notification would place an undue hardship upon the entity making notice of a data security breach. The issue here is not so much the availability of the safe harbor provision as its questionable benefit. Companies that fall within the protection of the large breach exemption must consider whether a directed mailing is superior to taking out an advertisement in the newspaper, regardless of the initial cost. The former only announces the problem to those affected, while the latter announces it to the world.

Typically, state breach laws confine themselves to events involving personally identifiable information

(PII); though often not defined in statutes, the conventional approach is that PII is non-public information from which a unique individual can be reasonably identified. Some of the more recently enacted state breach laws have taken PII a step further and added personal health care information (PHI), such that the statutes are no longer simply focused on financial identity theft. To some extent, this move came as a reaction to the Health Information Technology for Economic and Clinical Health Act (HITECH) amendment to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The HITECH amendment to HIPAA is the key federal statute that has caused the most concern recently. HITECH changed HIPAA in several ways, including:

- implementing new rules to account for disclosures of a patient's health information;
- amending and extending newly updated civil and criminal penalties to business associates;
- extending the complete privacy and security provisions of HIPAA to business associates of covered entities; and
- imposing new notification requirements on covered entities, business associates, vendors of personal health records (PHR) and related entities if a breach of unsecured PHI occurs.

The extension of HIPAA to business associates and other non-traditional health care firms has been particularly problematic for some commercial entities. This modification to the law has substantially widened its reach and potentially increased the risk associated with providing services to health care entities. Further, the ability to enforce HIPAA and its amendments has been expanded

such that state attorneys general can now bring an action pursuant HIPAA.

The single largest change from the passage of HITECH is the imposition of a duty on entities to notify individuals if their personal health information is breached, mishandled, or otherwise compromised in any way. This new duty also comes with a requirement that if the breach is of a certain size—500 or more records—the entity must alert the Department of Health and Human Services. The HITECH notification duty does, however, come with an “escape clause.” The statute allows for a likelihood of harm analysis before the duty of notification attaches. Notice, under the statute, need only be provided if the data breach creates “a significant risk of financial, reputational, or other harm to the individual.”

In addition to the aforementioned state breach laws and HITECH/HIPAA, the most recent development in the state privacy law realm has been the passage of several laws meant to mirror the “Red Flags Rule” promulgated by the Federal Trade Commission (FTC). These laws essentially mandate that commercial entities that hold personal information about a states’ citizens (with respect to the “Red Flags Rule” the personal information is credit information) have an incident response plan in place. This latest variant of privacy law is meant to be a bit more pro-active in that the entity is now being told that it must have a privacy disaster plan as well as what that plan must entail.

On the international front, there has recently been movement in Canada, Europe, and the United Kingdom toward adoption of privacy breach notice legislation. In addition to the federal Personal Information Protection and

Electronic Documents Act (PIPEDA), which does allow for privacy breach notice at the discretion of the Privacy Commissioner, Canada has at least one provincial regulation requiring notice if PII is disclosed or mishandled. There are also Canadian regulations that address the necessity of notice in situations involving the disclosure or mishandling of PHI. In Europe, the European Union (EU) Data Protection Directive focuses not so much on a data security breach, but on the general handling and use of personal information. Two countries—Germany and Austria—have recently drafted legislation that would create a breach notification requirement. The United Kingdom has run hot and cold on the issue, alternately decrying such legislation, only to embrace and call for EU-wide legislation.

Overall, governments continue to maintain an aggressive stance relative to privacy regulation. In fact, the FTC recently publicly supported the development of a “do not track” tool that would enable people to avoid having their actions monitored on-line. Although the advertising industry was up in arms, the FTC advised that self-regulation relative to web privacy was failing, and that the FTC was merely making recommendations at this juncture. Companies are well advised to keep apprised of these developments and all facets of this fast evolving area of the rules and the law, where even simple compliance can be a complicated and expensive proposition. #

For more information about this topic, please contact your FINPRO representative or the author of this article, Robert Parisi, Robert.Parisi@marsh.com, (212) 345-5924.

Employment Practices Liability: The Good, the Bad and the Ugly—A Year in Review

By Adeola I. Adele, Marsh FINPRO
Employment Practices Liability
Product Leader

As 2010 comes to a close, risk managers and insurers alike await the outcomes of a number of court cases that may affect the employment practices (EPL) liability insurance market in 2011. For example, on December 6, 2010, the world's largest retailer learned that the U.S. Supreme Court will hear its appeal in the estimated \$1 billion gender discrimination lawsuit filed over a decade ago by six female employees on behalf of over 1.5 million female employees. A decision is expected by the Supreme Court in June 2011. Additionally, final approval of a \$175 million settlement (following a historic \$250 million punitive damages verdict in May 2010) in a gender discrimination class action brought against a U.S. unit of a Swiss pharmaceutical company is imminent.

This judicial activity, coupled with the skyrocketing wage and hour collective actions, is the foundation against which EPL class action trends have been measured. While significant, these trends were not the only EPL headlines nor newsworthy events of 2010. This article reviews the top EPL issues risk managers faced in 2010 and provides insight for the year ahead.

Unemployment and the EEOC

Despite double-digit job gains in various industries, the national unemployment rate has lingered around 9.6 percent since May 2010. The unemployment rate is a strong indicator that companies continue to conduct layoffs or are otherwise reducing their workforce in an effort

to manage the costs and effects of the recession. Just as companies are looking for ways to deal with the slowly recovering economy, so are the unemployed; thus compounding today's growing EPL risks. According to the U.S. Equal Employment Opportunity Commission (EEOC) Fiscal Year 2010 Performance and Accountability Report, the number of private sector charges of discrimination filed with the agency in 2010 is 99,922, an increase of 7 percent over the 93,277 charges filed in 2009. The 2010 percentage increase

discrimination lawsuit against past or prospective employers.

The increase in employment claims can in part be attributed to the additional funding provided to the EEOC in 2010 and the estimated additional funding for 2011. This funding has enabled claimants to file charges of discrimination via the Internet. It has also permitted the EEOC to hire additional personnel to facilitate charge processing, as well as pursue litigation involving systemic discrimination, which remains the agency's priority.



is higher than any previous year, with the exception of the 15.2 percent increase in 2008.

Studies have consistently shown that there is a correlation between the unemployment rate and an increase in employment-related claims. Retaliation claims, which are on the rise, are particularly common from disgruntled employees who have been terminated from employment. Further, older workers who are experiencing difficulty re-entering the workforce may surmise that their only option is to bring an age

The Benefits and Curse of Social Networking

Compounding the EPL exposure is the increasing popularity and use of social networking websites by employees. In this regard, Facebook announced in July 2010 that it reached the 500 million users mark, reportedly making it the third largest "country" in the world. Use of social networking websites during work hours (and non-work hours) has already led to claims of discrimination, wrongful termination, retaliation, invasion of privacy, and defamation by employees,

as well as claims by non-employees (i.e., third parties) based on the conduct of employees. This exposure is illustrated by a recent lawsuit filed by the National Labor Relations Board (NLRB) on behalf of a union employee who was allegedly wrongfully terminated after she posted—from her home computer—negative remarks on her Facebook page about her supervisor. According to the NLRB, the employer's Internet usage policy is illegal and "overly broad" because it silenced employees and denied them the right to engage in a "protected concerted activity."

In addition to employees, companies create their own exposure as a result of their social networking activities. Many corporations now use social networking websites as part of their background checks of potential job applicants and as a means to monitor employees' productivity or on-the-job activities. Although these practices may be beneficial, they are also fraught with EPL risks. As such, companies using information obtained from social networking websites about applicants for employment or current employees must be cognizant that they will be held to greater scrutiny and likely be required to prove that the information obtained is job-related. Therefore, it is critical to create and implement unambiguous Internet usage policies as well as educate/train supervisors and managers in an effort to minimize this growing EPL exposure.

Obama's Employment Law Agenda

As a result of the 2010 mid-term elections, 2011 is likely to be an uneventful year for the Obama Administration's legislative agenda for employment law issues. On November 17, 2010, the Paycheck Fairness Act failed to secure the necessary 60 votes in the Senate; the final vote was 58-41. The Act, among other provisions, would have: (1) allowed the EEOC to collect compensation data from employers; (2) eliminated the caps on compensatory and punitive damages; and (3) prohibited retaliation against employees who share salary information with other employees. Similarly, the Employee Free Choice Act—a pro-union bill and a priority on Obama's legislative agenda—is likely to be stalled in a "lame duck" session, if not entirely abandoned. The Employment Non-Discrimination Act, which prohibits discrimination in employment on the basis of gender identity and sexual orientation, is also likely to suffer a similar fate.

One bill that may survive the divided executive and legislative branches is the Employee Misclassification Act—a bill intended to prevent the misclassification of workers as independent contractors instead of employees—because of the fines and penalties to be collected by the Internal Revenue Service from offending employers.

Looking Ahead to 2011

In addition to federal legislation, state anti-discrimination laws continue to expand to afford employees greater rights and protection than those available under federal laws. Further, given the current composition of Congress, the EEOC and state administrative agencies are likely to be even more protective of employees and determined to litigate perceived violations of employee rights under existing anti-discrimination statutes. Companies are well advised to remain proactive in assessing and enforcing their employment practices policies and procedures, particularly regarding pay equity and retaliation issues.

Finally, contrary to current conditions, the EPL insurance market is still experiencing a "buyer's" market: many of Marsh's clients have received premium rate reductions between 5 percent and 10 percent. This soft market is largely driven by an abundance of capacity, competition, and unripened claims. Therefore, barring any catastrophic loss or exit of one or more major insurers from the market, EPLI premium rates are likely to remain "soft" through the first quarter of 2011. #

For more information on this topic, please contact the author of this article, Adeola I. Adele at Adeola.I.Adele@marsh.com, (212) 345-1724 or your FINPRO representative.

The information contained in this publication is based on sources we believe reliable, but we do not guarantee its accuracy. This information provides only a general overview of subjects covered; is not intended to be taken as advice regarding any individual situation or as legal, tax, or accounting advice; and should not be relied upon as such. Recipients of this publication should consult their own insurance, legal, and other advisors regarding specific coverage and other issues.

Marsh is part of the family of MMC companies, including Guy Carpenter, Mercer, and the Oliver Wyman Group (including Lippincott and NERA Economic Consulting). This document or any portion of the information it contains may not be copied or reproduced in any form without the permission of Marsh Inc., except that clients of any of the MMC companies need not obtain such permission when using this report for their internal purposes, as long as this page is included with all such copies or reproductions.

Copyright © 2010 Marsh Inc. All rights reserved. Compliance No. : MA10-10384 December 2010

*Note: When viewing electronically, this document is interactive. [Text appearing in this format](#) indicates active links that may be clicked on for additional information.