Preventive Measures in a New Age: Preparing for New Technology and New Statutes *

Theodore L. Banks
Scharf Banks Marmor LLC
333 W. Wacker Dr.
Chicago, IL 60606
Tbanks@ScharfBanks.com
312-662-4897

1. Introduction

a. Advising your client on the employment law legal risks is not a static process. New laws, at the state, federal, and even local level may impose additional obligations on employers which can impose "gotcha" liability if you aren't vigilant. And those laws do not always proclaim that they are employment laws. Sometimes, like Dodd-Frank, they are laws apparently aimed at one industry (like finance) that contain new employment law rules of more general application.

b. In addition, you need to be sensitive to social and technological changes, and constantly consider how those changes impact on people's lives, since they bring their lives with them to work – and they take their work home with them. With the constant availability of computer connections through smart phones, and the trend to constant communications through Facebook and other social networking sites, the line between what is done on the job and what is private life is blurred – at least to some people. Can you "unblur" it? Should you?

2. The Compliance Program

a. The compliance program starts with a risk assessment where you rank the legal risks facing the company by severity and likelihood of occurrence.

1) A partial list of the employment-related laws to worry about include the following: Age Discrimination in Employment Act, Americans with Disabilities Act, Child Labor Laws, Fair Labor Standards Act, Civil Rights Act of 1964, Executive Order 11246 (1965), Employee Polygraph Protection Act of 1988, Family and Medical Leave Act, independent contractor status, Immigration

---

* Portions adapted from T. Banks (ed.), Corporate Legal Compliance Handbook (2d. ed. 2011), published by Wolters Kluwer/Aspen Law & Business.

Reform and Control Act of 1986, Sexual Harassment, Uniformed Services Employment and Reemployment Rights Act of 1994, Worker Adjustment Retraining and Notification Act of 1988, whistleblowing laws – and more.

2) In addition to the conventional legal risks, one should also look for changed circumstances since the last risk assessment, which may include new laws, new regulations, new businesses, and new technology.

3) The Dodd-Frank law, and the development of pervasive use of social media, as discussed below, are two changes in the risk environment that a company should evaluate to determine what kind of compliance program is appropriate.

b. After the company has identified and prioritized its key compliance risks, it must then develop a program to mitigate those risks. The compliance program generally consists of two main focused efforts: employee education and business controls.

1) Employee education is designed to make certain that employees understand their responsibilities to abide by the law, and the consequences if they fail to do so.

2) Business controls, implemented where possible, are designed to make it difficult (or even impossible) for an employee to violate the law.

c. The Organizational Sentencing Guidelines of the United States Sentencing Commission[1] outline additional steps than an enterprise should take as part of its due diligence to ensure that it has an effective compliance program. An effective compliance program should, at a minimum, have the following components:

1) Standards and procedures are implemented to prevent and detect criminal conduct

2) Senior management is responsible to ensure that the compliance program is effective and has adequate resources

3) Specific individuals have implementation authority

4) People who have engaged in misconduct will not be given senior management positions

5) Compliance program elements are communicated to employees, with training as appropriate to an employee's responsibilities

6) The program will be monitored and audited

7) There is a reporting mechanism that will allow for anonymous reports of wrongdoing

---

[1] http://www.ussc.gov/Guidelines/Organizational_Guidelines/index.cfm

8) Incentives for compliance, and punishment for noncompliance

9) There is a prompt response to allegations of wrongdoing, and the compliance program is modified as appropriate

3. Dodd-Frank

a. The Dodd-Frank Wall Street Reform and Consumer Protection Act[2] was passed after the massive financial meltdown that began in 2008. The law is huge,[3] and while most of the provisions were directed at the financial markets,[4] there are a variety of provisions that may impact businesses outside of the financial area.[5] Of particular interest to compliance officers, human resources staff, and employment lawyers, § 922 of the Act authorizes the SEC to pay rewards to individuals who provide the Commission with original information that leads to successful SEC enforcement actions. Prior to the passage of the law, the agency's bounty program was limited to insider trading cases, with an award cap of 10 percent of the penalties collected. The potential payout is now increased to up to 30 percent of the recovery by the SEC, if it recovers over $1 million.[6]

b. The whistleblower rules adopted by the SEC[7] provisions define a whistleblower as a person who provides information to the SEC relating to a possible violation of the securities laws (past, present or future). To qualify for an award, the whistleblower must voluntarily provide information to the government, a self-regulatory organization or the Public Company Accounting Oversight Board (PCAOB). It will still be considered voluntary if the information is provided as a result of a request from the PCAOB.

---

[2] Dodd–Frank Wall Street Reform and Consumer Protection Act, Pub.L. 111-203, H.R. 4173, signed into law on July 21, 2010.

[3] 849 pages, compared to the 66 pages of Sarbanes-Oxley.

[4] The SEC and CFTC were mandated to issue rules in dozens of areas governing various financial instruments and practices.

[5] For example, § 342 requires thirty federal financial agencies and departments to establish an Office of Minority and Women Inclusion. Each such office will be headed by a director, who will be responsible for "develop[ing] and implement[ing] standards and procedures to ensure, to the maximum extent possible, the fair inclusion and utilization of minorities, women, and minority-owned and women-owned businesses in all business and activities of the agency at all levels, including in procurement, insurance, and all types of contracts." Anyone bidding on federal service contracts will need to provide a written statement, "in a form and with such content as the Director shall prescribe," that the contractor will undertake efforts, "to the maximum extent possible," to ensure the fair inclusion of women and minorities in its workforce and, if applicable, in the workforce of its subcontractors. Failure to make a "good faith effort to include women and minorities" in the workforce shall result in a recommendation from the director that the contract be terminated.

[6] Multiple cases that arise out of a common set of facts may be aggregated to reach the $ 1 million threshold.

[7] Section 922(a) of Dodd-Frank became § 21F of the Securities Exchange Act. Regulation 21F was adopted May 25, 2011, effective August 12, 2011.

c. The information must be "original," that is, based on the whistleblower's independent knowledge or independent analysis, not already known to the SEC, and not derived exclusively from certain public sources. If this original information is reported to a company's internal reporting system, the whistleblower will get credit for all information that is provided by the company to the SEC, including information generated by the company and not provided by the whistleblower. The payout occurs if there has been a successful enforcement by the SEC in a federal court or administrative action, and the information is sufficiently specific, credible and timely to cause the Commission to open a new examination or investigation, reopen a closed investigation, or open a new line inquiry in an existing examination or investigation. If the conduct was already under investigation when the information was submitted, the information must significantly contribute to the success of the action.

d. Corporations were concerned about their compliance programs being undermined by providing incentives to report to the government without first reporting the concerns internally.[8] The SEC did not agree to require internal reporting, but it did allow that internal reporting would be considered as a factor that might increase the award to the whistleblower; interference with internal investigations could decrease the award. The date the whistleblower makes an internal report will be deemed to be the date of a report to the SEC, so long as the whistleblower or the company subsequently reports the information to the SEC within 120 days of the initial internal report. Notwithstanding the absence of any requirement to report internally first, companies should continue to emphasize the importance of reporting any suspected wrongdoing to the internal avenues that are available.

e. Some people will be excluded from the whistleblower bounty provisions, such as:

1) People who have a pre-existing legal or contractual duty to report their information to the SEC;

2) Attorneys (including in-house counsel) who attempt to use information obtained from client engagements to make whistleblower claims for themselves (unless disclosure of the information is permitted under SEC rules or state bar rules);

3) officers, directors, trustees or partners of an entity who are informed by another person (such as by an employee) of allegations of misconduct, or who learn the information in connection with the entity's processes for identifying, reporting and addressing possible violations of law (such as through the company hotline);

4) Anyone who obtains the information by means or in a manner that is determined by a U.S. court to violate federal or state criminal law;

5) Compliance and internal audit personnel;

[8] The concerns continue, and a bill has been introduced in Congress to require internal reporting.

6) Public accountants working on SEC engagements, if the information relates to violations by the engagement client; and

7) Foreign government officials,

f. Notwithstanding the exclusions outline above, compliance officers, internal auditors, and public accountants could qualify for a whistleblower bounty

1) If they make a disclosure under the belief that it may prevent substantial injury to the financial interest or property of the entity or investors, or

2) The whistleblower believes that the entity is engaging in conduct that will impede an investigation, or

3) at least 120 days have elapsed since the whistleblower reported the information to his or her supervisor or the entity's audit committee, chief legal officer, chief compliance officer, or

4) at least 120 days have elapsed since the whistleblower received the information, if the whistleblower received it under circumstances indicating that the audit committee, chief legal officer, or chief compliance were already aware of the information.

g. People who are deemed culpable and pay a fine to the SEC cannot recover a bounty, nor can whistleblowers recover if monetary sanctions were paid by an entity where liability was based substantially on conduct that the whistleblower directed, planned or initiated. Employees of certain agencies and people who are convicted of violating the law based on the conduct they report, cannot recover a bounty.

h. As with Sarbanes-Oxley (SOX), whistleblowers are protected from retaliation if there is a reasonable belief that the information relates to a possible securities law violation that has occurred, is ongoing, or is about to occur. It is unlawful for anyone to interfere with a whistleblower's efforts to communicate with the SEC, including threatening to enforce a confidentiality agreement. Employers may not retaliate against whistleblowers "because of any lawful act done by the whistleblower" when he or she provides information to the SEC, participates in an SEC investigation or action based on information provided by the whistleblower, or makes disclosures required by SOX and any other law, rule, or regulation subject to the jurisdiction of the SEC.[9]

i. The "clawback" provisions of SOX § 304 have been expanded by § 954 of Dodd-Frank. The new statute requires a company that restates its earnings to recover any excess incentive-based compensation given to any current or former executive officer in the last three years, even if the compensation was received inadvertently. From a compliance standpoint, this suggests that incentive-based compensation programs might contain a provision that would automatically retrieve compensation in the event of an earnings restatement.

---

[9] Reg. 240.21F-2(b)(ii).

j. Employees are most likely to report internally first when they feel they can trust the reporting system. Make certain that there is a strong "no retaliation" policy. Make certain that any complaint that is received is promptly investigated.

4. Social Media

a. All of a sudden, it is pervasive. This development is somewhat parallel to the rise of e-mail in the corporate environment: it was used by computer departments, fairly quietly, and then, all of a sudden, everyone was using it. Inappropriate things were said, people were copied when they shouldn't have been, company secrets were revealed, e-mails were not produced in discovery when they should have been, it became a great time-waster on the job, and sometimes it was used to harass or annoy other employees.

b. Social media reinforces the notion that one wants to share every detail of life with all of one's "friends." And with the use of smartphones and computers at work that have Internet access, that sharing can go on constantly, with blurring between what is work-related and should stay at work, and what is personal information that can be shared based on the whims of the owner.

1) Employees should be educated about what business subjects are the proper topics for discussion on social media. (See sample policy from Intel below)

2) Some companies may want to prohibit any mention of the company, but this is probably unnecessarily restrictive and misses the chance to use the employee as a booster. And it may run into the NLRB that doesn't view these restraints kindly (see NLRB memo and sample policy below)

3) Employees should be educated that their actions on social media sites may have implications for their jobs. They need to understand the risks of certain conduct on social media sites, such as defamation or violation of intellectual property rights. Again, the government's position in this area needs to be considered.

4) Employees should also understand that they may hurt their employer by revealing proprietary or inaccurate information.

5) Employees should understand that they should not make claims about themselves that are not true, or contradict things that they told their employer.

c. Companies may want to use social media affirmatively to promote their products or manage their business.

1) Employers may want to examine social media sites to learn about employees before hiring, but beware. This is becoming part of the normal pre-employment due diligence that has become accepted post 9-11. But the tension between

protection of privacy and the imperative to perform pre-employment background checks has not been resolved. Although an employer is generally allowed to take action against an employee where his or her off-duty activities damaged the company, there are limits to what can be done with information discovered on line.

a) Cannot use social media to ask questions that would be improper in an interview (e.g., protected class, health information)

b) About 30 states have enacted statutes that prohibit employers from taking action against employees based on consumption of legal products (i.e., tobacco and alcohol) while off duty.

c) Four states have statutes that restrict the actions an employer can take based on an employee's lifestyle

2) Although an employer can – in general -- control and monitor an employee's computer use while on the job, it should not gain access to an employee's social media account without authorization.

3) If a company wishes to promote itself through social media (i.e., its securities, as opposed to its products), it must follow the applicable securities law rules. See the FINRA notice below.

4) If a company wishes to promote a regulated product (e.g., pharmaceutical) through social media, it must follow all of the requirements that would apply through other media (e.g., communication of risks along with benefits)

5) It is a good idea to monitor social media to learn about business problems that might require a response on-line or corrective action

6) Discovery of content in social media sites in an important part of litigation, but do not use deception to obtain nonpublic material

7) Notwithstanding the sensibility of many of these rules, the NLRB takes a rather slanted approach.[10] For example:

a) Confidentiality:
Illegal: A policy that prohibits the "release [of] confidential guest, team member or company information".
Legal: A policy that cautions employees to be suspicious when asked to disclose confidential information.

b) Copyright:
Illegal: "Get permission before reusing others' content or images".

[10] Thanks to Doug Cornelius and the "Compliance Building" blog (6/3/2012)

Legal: "Respect all copyright and other intellectual property laws."

c) Offensive or abusive language:
Illegal: "Offensive, demeaning, abusive or inappropriate remarks are as out of place online as they are offline"
Legal: "Employees should avoid harming the image and integrity of the company and any harassment, bullying, discrimination, or retaliation that would not be permissible in the workplace is not permissible between co-workers online, even if it is done after hours, from home and on home computers".

d) Accuracy:
Illegal: Requiring employees to be "completely accurate and not misleading".
Legal: "Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly."

e) Non-Public information
Illegal: "Do not reveal non-public information on any public site."

f) Savings clause
"This policy is for the mutual protection of the company and our employees, and we respect an individual's rights to self-expression and concerted activity. This policy will not be interpreted or applied in a way that would interfere with the rights of employees to self-organize, form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, or to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection or to refrain from engaging in such activities.
Illegal: a savings clause "does not cure the ambiguities in a policy's otherwise unlawful provisions."

d. Bottom Line: If you are involved in a labor dispute, be very careful about what kind of social media policy you implement. Sticking closer to the NLRB's suggested policy, even if the original policy was reasonable, may remove one issue that can be used against the company in a labor dispute.

Sample Materials

Intel Social Media Guidelines

http://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html

These are the official guidelines for social media at Intel. If you're an Intel employee or contractor creating or contributing to blogs, wikis, social networks, virtual worlds, or any other kind of social media both on and off intel.com—these guidelines are for you. We expect all who participate in social media on behalf of Intel to be trained, to understand and to follow these guidelines. Failure to do so could put your future participation at risk. These guidelines will continually evolve as new technologies and social networking tools emerge—so check back once in awhile to make sure you're up to date.

When You Engage

Emerging platforms for online collaboration are fundamentally changing the way we work, offering new ways to engage with customers, colleagues, and the world at large. It's a new model for interaction and we believe social computing can help you to build stronger, more successful business relationships. And it's a way for you to take part in global conversations related to the work we are doing at Intel and the things we care about.

If you participate in social media, please follow these guiding principles:

- Stick to your area of expertise and provide unique, individual perspectives on what's going on at Intel and in the world.
- Post meaningful, respectful comments—in other words, no spam and no remarks that are off-topic or offensive.
- Always pause and think before posting. That said, reply to comments in a timely manner, when a response is appropriate.
- Respect proprietary information and content, and confidentiality.
- When disagreeing with others' opinions, keep it appropriate and polite.
- Know and follow the Intel Code of Conduct and the Intel Privacy Policy.

Rules of Engagement

Be transparent. Your honesty—or dishonesty—will be quickly noticed in the social media environment. If you are blogging about your work at Intel, use your real name, identify that you work for Intel, and be clear about your role. If you have a vested interest in something you are discussing, be the first to point it out. Transparency is about your identity and relationship to Intel. You still need to keep confidentiality around proprietary information and content.

Be judicious. Make sure your efforts to be transparent don't violate Intel's privacy, confidentiality, and legal guidelines for external commercial speech. Ask permission to publish or report on conversations that are meant to be private or internal to Intel. All statements must be true and not misleading and all claims must be substantiated and approved. Product benchmarks must be approved for external posting by the appropriate product benchmarking team. Please

never comment on anything related to legal matters, litigation, or any parties we are in litigation with without the appropriate approval. If you want to write about the competition, make sure you know what you are talking about and that you have the appropriate permission. Also be smart about protecting yourself, your privacy, and Intel Confidential information. What you publish is widely accessible and will be around for a long time, so consider the content carefully.

Write what you know. Make sure you write and post about your areas of expertise, especially as related to Intel and our technology. If you are writing about a topic that Intel is involved with but you are not the Intel expert on the topic, you should make this clear to your readers. And write in the first person. If you publish to a website outside Intel, please use a disclaimer something like this: "The postings on this site are my own and don't necessarily represent Intel's positions, strategies, or opinions." Also, please respect brand, trademark, copyright, fair use, trade secrets (including our processes and methodologies), confidentiality, and financial disclosure laws. If you have any questions about these, see your Intel legal representative. Remember, you may be personally responsible for your content.

Perception is reality. In online social networks, the lines between public and private, personal and professional are blurred. Just by identifying yourself as an Intel employee, you are creating perceptions about your expertise and about Intel by our shareholders, customers, and the general public-and perceptions about you by your colleagues and managers. Do us all proud. Be sure that all content associated with you is consistent with your work and with Intel's values and professional standards.

It's a conversation. Talk to your readers like you would talk to real people in professional situations. In other words, avoid overly pedantic or "composed" language. Don't be afraid to bring in your own personality and say what's on your mind. Consider content that's open-ended and invites response. Encourage comments. You can also broaden the conversation by citing others who are blogging about the same topic and allowing your content to be shared or syndicated.

Are you adding value? There are millions of words out there. The best way to get yours read is to write things that people will value. Social communication from Intel should help our customers, partners, and co-workers. It should be thought-provoking and build a sense of community. If it helps people improve knowledge or skills, build their businesses, do their jobs, solve problems, or understand Intel better—then it's adding value.

Your Responsibility: What you write is ultimately your responsibility. Participation in social computing on behalf of Intel is not a right but an opportunity, so please treat it seriously and with respect. If you want to participate on behalf of Intel, take the Digital IQ training and contact the Social Media Center of Excellence. Please know and follow the Intel Code of Conduct. Failure to abide by these guidelines and the Intel Code of Conduct could put your participation at risk. Contact social.media@intel.com for more information. Please also follow the terms and conditions for any third-party sites.

Create some excitement. As a business and as a corporate citizen, Intel is making important contributions to the world, to the future of technology, and to public dialogue on a broad range of

issues. Our business activities are increasingly focused on high-value innovation. Let's share with the world the exciting things we're learning and doing—and open up the channels to learn from others.

Be a Leader. There can be a fine line between healthy debate and incendiary reaction. Do not denigrate our competitors or Intel. Nor do you need to respond to every criticism or barb. Try to frame what you write to invite differing points of view without inflaming others. Some topics—like politics or religion—slide more easily into sensitive territory. So be careful and considerate. Once the words are out there, you can't really get them back. And once an inflammatory discussion gets going, it's hard to stop.

Did you screw up? If you make a mistake, admit it. Be upfront and be quick with your correction. If you're posting to a blog, you may choose to modify an earlier post—just make it clear that you have done so.

If it gives you pause, pause. If you're about to publish something that makes you even the slightest bit uncomfortable, don't shrug it off and hit 'send.' Take a minute to review these guidelines and try to figure out what's bothering you, then fix it. If you're still unsure, you might want to discuss it with your manager or legal representative. Ultimately, what you publish is yours—as is the responsibility. So be sure.

Contractors & Endorsements

Intel supports transparency. We are committed to ensuring that our social media practitioners (including blogs, Twitter*, forums and any other social media) clearly disclose relationships and endorsements, and that statements about Intel products are truthful and substantiated.

Please remember that any social media experts contracted, seeded or in any way compensated by Intel must follow the Intel Sponsored, Seeded or Incentivized Social Media Practitioner Guidelines. As part of these guidelines, you need to disclose that you have been seeded or otherwise compensated by Intel. Your blog will be monitored for compliance with our guidelines and accurate descriptions of our products and claims.

Moderation Guidelines

Moderation is the act of reviewing and approving content before it's published on the site (This applies to social media content written on behalf of Intel, whether the site is on or off intel.com). Intel does not endorse or take responsibility for content posted by third parties, referred to as user generated content (UGC). This includes text input and uploaded files (video, images, audio, executables, and documents).

While we strongly encourage user participation, there are some guidelines we ask you to follow to keep it safe for everyone. In addition, Intel has put in place automated controls to combat spam and malicious content. Please note that content originating inside Intel is not moderated. This means we allow our blog authors to post directly without approval, as long as they have taken the required trainings.

Pre-moderation. Even when a site requires the user to register before posting, simple user name and email entry doesn't really validate the person. So to ensure least risk/most security, we require moderation of all UGC posts before they are published (pre-moderation).

Community moderation. For established, healthy communities, group moderation by regular users can work well. This will sometimes be allowed to take the place of pre-moderation—it must be applied for and approved.

Balanced online dialogue. Whether content is pre-moderated or community moderated, follow these three principles: the Good, the Bad, but not the Ugly. If the content is positive or negative and in context to the conversation, then we approve the content, regardless of whether it's favorable or unfavorable to Intel. But if the content is ugly, offensive, denigrating and completely out of context, then we reject the content.

Last updated: March 2010

Guide to the Web for Registered Representatives

Introduction

FINRA has developed this page to make registered representatives (RRs) aware of the compliance requirements and potential liabilities when using the Web and electronic communications for business purposes.

This page addresses some general compliance requirements that apply to electronic communications. It also discusses specific considerations relating to the use of email, instant messaging and websites including social networking sites, chat rooms, blogs, bulletin boards as well as the use of personal devices. We have based the information on published rules, interpretations and notices. Wherever possible, a link to the actual text of the rule or interpretation is provided.

An RR's compliance responsibilities when communicating via the Web or other electronic media are the same as in face-to-face discussions or in written communications with the public. In addition, RRs must be aware of internal firm policies and procedures that may restrict or prohibit the use of electronic communications.

Categories of Electronic Communications with the Public

Electronic communications may fall under any one of categories of communications defined in FINRA's advertising rules. FINRA has provided detailed guidance on social media communications and websites in Regulatory Notice 10-06 and Regulatory Notice 11-39. Information on these and related advertising compliance issues can be found on the Advertising Regulation Web page. In general:

- Publicly available websites, banner advertisements, and bulletin boards are considered advertisements. Static (non-interactive) content on social networking sites and blogs are also deemed to be an **advertisement**.
- An email or instant message sent to 25 or more prospective retail customers is considered **sales literature**.
- An email or instant message is considered **correspondence** if it is sent to: i) a single customer (prospective or existing); ii) an unlimited number of existing retail customers and/or less than 25 prospective retail customers (firm-wide) within a 30-day period.
- Password-protected websites are considered **sales literature**.
- Content posted in a real-time interactive electronic forum (including extemporaneous chat room, social networking and blog comments) is considered a **public appearance**.

Rules that Affect Electronic Communications

All communications with the public are subject to compliance with FINRA rules and related interpretative materials. Set forth below are highlights of the rules that apply to all forms of electronic communications. RRs are urged to view the actual rules using the links provided.

Standards of Commercial Honor and Principles of Trade (FINRA Rule 2010)

Rule 2010 requires RRs to adhere to high standards of commercial honor and just and equitable principles of trade in conducting their business. Guidance regarding compliant ways to transact business and ensure just and equitable principles of trade are addressed in Interpretive Material related to this rule.

Communications with the Public (NASD Rule 2210)

Communications with the public must:

- be based on principles of fair dealing and not omit material information, particularly risk disclosure;
- not make exaggerated, unwarranted, or misleading claims;
- give the investor a sound basis for evaluating the facts in regard to any particular security, type of security, industry or service;
- not contain predictions or projections of investment results; and
- identify the name of the member firm.

Guidelines to Ensure Communications With the Public are Not Misleading (IM-2210-1)

IM-2210-1 makes it clear that every member is responsible for determining whether any communication with the public is compliant. It also addresses what must be considered in determining whether a communication complies with all applicable standards.

Recordkeeping (SEC Rule 17a-4, NASD Rule 2210(b) and NASD Rule 3110(a)[1])

In accordance with SEC Rule 17a-4, firms must retain all incoming and outgoing communications related to their firms business as such. Also, under NASD Rules 2210 and 2211, firms must retain all communications for a period of three years from the date of last use. For example, if an RR maintains a business-related web site, all information posted on the site must be captured and retained by the broker dealer. Similarly, any business-related email, instant messages or postings on a social media site must also be captured and retained by the broker dealer. RRs must know and comply with their firm's policies and procedures with respect to record keeping. If an RR's firm permits the use of personal devices such as a smart phone for firm business communications, the firm must be able to retain, retrieve and supervise business communications.

Approval and Supervision (NASD Rules 2210(b) and 3010)

Web communications that meet the definitions of advertisements, sales literature or independently prepared reprints set forth in NASD Rule 2210(a) must be approved prior to use and in writing by a registered principal of the broker dealer. For example, a website or search engine advertisement must be approved before use. In addition, the rules require that correspondence (which can include email and instant messages) distributed to more than 25 individuals within a 30-day period also receive prior-to-use principal approval. For example, an email message that contains a recommendation of a security and is distributed to more than 25 existing clients must be approved. Firms may employ an electronic system to capture and document these approvals.

In contrast, email or instant messages distributed to 25 or fewer individuals may be supervised in accordance with written policies and procedures developed by the firm. Regulatory Notice 07-59 provides detailed guidance to firms about how to supervise this type of electronic correspondence. Your firm may require that all of your electronic correspondence be approved prior to use and in writing, or your firm may audit your electronic correspondence using systems and controls it has developed. You should be aware of your firm's policies with respect to electronic correspondence and ensure that you follow them at all times.

FINRA has also provided guidance about how firms can supervise interactive electronic communications by representatives using social media websites such as blogs or social networking sites (see Regulatory Notice 10-06 and 11-39). The firm must review prior to use any social media site that the RR intends to employ for a business purpose in the form in which the site will be "launched." In addition, some communications on social media sites are considered advertisements that must be approved prior to use and in writing, while other communications may be considered public appearances that can be supervised in accordance with procedures adopted by your firm. For example, static content such as profile information on a social networking site or a blog posting will generally be considered an advertisement that requires firm approval before use. In contrast, your firm may choose to treat interactive comments posted in response to other comments by an unrelated third party as a public appearance. As such, the firm may

choose to allow such comments to be approved after use. As this is an area of firm supervision, you must get the approval of your compliance department and learn the appropriate policies and procedures before engaging in business use of a social media site.

Suitability: Recommendations to Customers (NASD Rule 2310)[2] and Online Communications (NASD Notice to Members 01-23)

RRs must have a reasonable basis for believing that each recommendation to a customer is suitable based on the information provided by the customer. To this end, RR's should make reasonable efforts to obtain information concerning a customer's financial status, tax status, investment objectives and other pertinent information considered reasonable in making a recommendation to the customer.

Notice to Members 01-23 addresses the applicability of suitability standards to electronic communications and clarifies what constitutes a recommendation in this environment. In this regard, RRs should note that the suitability rule fully applies to online activities where securities are recommended to customers. The Notice also offers examples of electronic activities that may fall outside the definition of a recommendation. Regulatory Notice 10-06 also makes clear these standards apply to social media participation.

Conflicts of Interest (NASD Rule 2711, IM-2210-1 (6)(C) and Regulatory Notices 07-04, 04-18 and 03-44)

RRs must avoid any conflicts of interest in transactions with customers. Rule 2711, IM-2210-1 (6)(C) and Notices 07-04, 04-18 and 03-44 cover conflict of interest issues regarding equity research reports and recommendations. Whether or not communicated electronically, conflict of interest and other disclosures required in research reports and recommendations must be made. RRs should note that they must not publish an equity research report without having registered as a research analyst and maintaining related continuing education requirements. Also, FINRA would give close scrutiny to circumstances where an RR personally buys shares of a thinly traded stock and then publicly makes a buy recommendation, or promotes the stock on the Web.

Day Trading Rules (FINRA Rules 2270 and 2130)

Rules 2270 and 2130 apply to member firms, and as such, RRs that promote day trading strategies. Firms are required to furnish a risk disclosure statement to a non-institutional customer prior to opening an account for the customer. In addition, the firm will either have to (1) approve the customer's account for a day trading strategy, or (2) obtain from the customer a written agreement that the customer does not intend to use the account for day-trading purposes. As part of the account approval process, the firm is required to make a threshold determination that day trading is appropriate for the customer. Regulatory Notices 09-72, 02-35 and 00-62, provide more information on these day-trading rules.

Electronic Communications Compliance Issues

EMail and Instant Messaging

RRs may mistakenly believe that sending an email or instant message from home through a personal account or from a personal device such as a smart phone or tablet computer exempts the communication from their firm's supervision or the regulations. In fact, whether sent from the office, home or elsewhere, email and instant messages that concern investments or a FINRA member firm's business fall under FINRA jurisdiction.

Group email and instant messages must be approved prior to use

In general, the same email or instant message sent to 25 or more prospective or existing customers within a 30-day period must be approved prior to use by an appropriately registered principal of the firm. Depending on their content, group messages may also require filing with FINRA's Advertising Regulation Department. Firms have flexibility to adopt their own procedures for how emails or instant messages sent to fewer than 25 individuals are handled. RRs should familiarize themselves with their firms' procedures and ensure they comply fully with them. RRs should contact their compliance departments for details in this area.

Firms must retain business-related email and instant messages

In addition to approval, firms must be able to retain and produce business related emails in accordance with specific regulations. RRs should familiarize themselves with their firms' requirements for email use and retention. For example, many firms require that all emails and instant messages be sent using firm equipment or software.

Web and Electronic Communications Compliance Issues:

The fact that an individual is registered subjects him/her to a higher standard than members of the general public. Given the fast-paced environment of electronic forums such as social media sites, chat rooms, blogs and bulletin boards, casual or off-handed statements have the potential of crossing the line from a reasonable opinion to a misleading, exaggerated or unwarranted claim.

Social Networking Sites and Chat Rooms

Social networking sites such as Facebook, Twitter and LinkedIn usually have static and interactive content. Static content like a profile, background or wall information is usually considered an "advertisement." Static content is generally accessible to all visitors and usually remains visible until it is removed. As with all advertisements and sales literature as defined, a registered principal for the firm must approve, prior to use, all static content. Interactive content includes real-time extemporaneous online discussions with unrelated third parties such as in a chat room. Chat room or other content posted in an interactive electronic forum is considered a public appearance. Similar to extemporaneous discussions by an RR at a public appearance, interactive content does not require prior principal approval, but must be supervised.

Blogs and Bulletin Boards

Blog and bulletin board postings by an RR are typically static communications. As with all advertisements and sales literature as defined, a registered principal for the firm must approve all static content. Blogs may also feature interactive content, where a third party posts a comment in response to the initial blog and then the blogger responds to the third party comment. Such interactive comments by the blogger are considered to be public appearances. Similar to extemporaneous discussions by an RR at a public appearance, the interactive content does not require prior principal approval, but must comply with the content standards of the advertising rules and must be supervised by the broker dealer.

Since interactive content in social networking sites and blogs is considered a public appearance, RRs must follow the same requirements for participating in these forums as they would if they were speaking in person before a group of investors. There are no filing requirements, but RRs are accountable under FINRA rules and the federal securities laws for what they say. Like all public communications, interactive electronic postings must be fair, balanced and not misleading.

RRs Must Contact their Compliance Department

Firms are responsible for supervising the business-related activities of RRs including participation in these interactive forums. The rules apply regardless of whether an RR is in the office, at home, on a public computer or using a personal device. Because of the difficulties of supervision and the potential liabilities from participating in these forums, many firms limit or prohibit participation in certain on-line media. Accordingly, RRs who are considering communicating in a social networking site, chat room, bulletin board or a blog, should contact their compliance department to determine whether such activities are permitted and what procedures may apply. Regulatory Notice 11-39 provides further guidance on accessing social media sites from personal devices.

In addition to Regulatory Notices 11-39 and 10-06 which provide the most recent written FINRA guidance on these issues, FINRA has also produced the following podcasts that also address the issues:

September 12, 2011
Social Media and Personal Electronic Devices – Part 1

September 19, 2011
Social Media and Personal Electronic Devices – Part 2

September 26, 2011
Social Media and Personal Electronic Devices – Part 3

Third Party Communications

Procuring Material from Third Party Websites

Sales communications sold at a third party site may not be compliant with the Rules, since such material may include misleading or dated information or be subject to filing with FINRA. Therefore, RRs should exercise extreme caution when procuring sales communications from a third party Web site.

Linking to Third Party Websites

Linking to other sites raises concerns because these sites may contain misleading or incorrect information. An RR's web site should not have a link to a site that he/she knows or has reason to know contains false or misleading content (see Regulatory Notices 10-06 and 11-39). RRs should exercise the same care in choosing links as they would in referring customers to any outside source of information.

Third Party Postings

Although third party postings (such as customer posts) on an RR's or firm's site are not treated as the firm's communication, RRs should exercise caution regarding a third party posting or link to the firm's social media site, especially if it is business-related. Content added to the site by a third party may be deemed the firm's communication if the firm had a role in creating it, endorsing it, or approving its use, as well as how the firm or the RR responds to the content. In addition, while the third party posts may not be deemed a communication of the broker dealer under FINRA's advertising rules, the firm will need to retain such information under SEC Rule 17a-4 if it relates to the firm's business and may have liability under other FINRA rules or the federal securities laws if such posting is fraudulent. Regulatory Notices 10-06 and 11-39 provide further guidance on this issue.

References to FINRA Membership and Linking to FINRA's Website

A firm or a person associated with the firm who refers to its membership within FINRA on a website must provide a hyperlink to FINRA's home page at www.finra.org. The hyperlink must be located in close proximity to the reference to FINRA membership. If more than one reference to FINRA membership is made on the website, the hyperlink may be placed in close proximity to any FINRA reference that is reasonably designed to draw the public's attention to FINRA membership.

There is no independent obligation requiring a member to mention its FINRA membership. Thus, the hyperlink is required only if a member or associated person of the member firm chooses to mention its membership on its website.

Please note that the use of FINRA 's logo on a firm's or RR's website is prohibited.

State Registration Requirements

Each state has separate registration requirements for individuals doing business in that state. Use of electronic communications may be deemed a solicitation of business. Generally, the solicitation of business in a state triggers the requirement for registration. RRs are advised to rely on their individual firms for guidance regarding state registration issues.

Other Pertinent FINRA Information for RRs:

- Broker Guidance & Information
- Disciplinary Information

---

1 Effective December 5, 2011, NASD Rule 3110, Books and Records, will be replaced by FINRA Rule 4511 as announced in Regulatory Notice 11-19.

2 Effective July 9, 2012, NASD Rule 2310 will be replaced by FINRA Rules 2090 and 2111. See Regulatory Notice 11-02.

September 26, 2011
Social Media and Personal Electronic Devices – Part 3

Last Updated: 9/21/2011

OFFICE OF THE GENERAL COUNSEL
Division of Operations-Management

MEMORANDUM OM 12-59 May 30, 2012

TO: All Regional Directors, Officers-in-Charge and Resident Officers

FROM: Anne Purcell, Associate General Counsel

SUBJECT: Report of the Acting General Counsel Concerning Social Media Cases

Attached is an updated report from the Acting General Counsel concerning recent social media cases.

/s/
A. P.

Attachment

cc: NLRBU
Release to the Public

REPORT OF THE GENERAL COUNSEL

In August 2011 and in January 2012, I issued reports presenting case developments arising in the context of today's social media. Employee use of social media as it relates to the workplace continues to increase, raising various concerns by employers, and in turn, resulting in employers' drafting new and/or revising existing policies and rules to address these concerns. These policies and rules cover such topics as the use of social media and electronic technologies, confidentiality, privacy, protection of employer information, intellectual property, and contact with the media and government agencies.

My previous reports touched on some of these policies and rules, and they are the sole focus of this report, which discusses seven recent cases. In the first six cases, I have concluded that at least some of the provisions in the employers' policies and rules are overbroad and thus unlawful under the National Labor Relations Act. In the last case, I have concluded that the entire social media policy, as revised, is lawful under the Act, and I have attached this complete policy. I hope that this report, with its specific examples of various employer policies and rules, will provide additional guidance in this area.

/s/
Lafe E. Solomon
Acting General Counsel

Rules on Using Social Media Technology and on Communicating Confidential Information Are Overbroad

In this case, we addressed the Employer's rules governing the use of social media and the communication of confidential information. We found these rules unlawful as they would reasonably be construed to chill the exercise of Section 7 rights in violation of the Act.

As explained in my previous reports, an employer violates Section 8(a)(1) of the Act through the maintenance of a work rule if that rule "would reasonably tend to chill employees in the exercise of their Section 7 rights." Lafayette Park Hotel, 326 NLRB 824, 825 (1998), enfd. 203 F.3d 52 (D.C. Cir. 1999). The Board uses a two-step inquiry to determine if a work rule would have such an effect. Lutheran Heritage Village-Livonia, 343 NLRB 646, 647 (2004). First, a rule is clearly unlawful if it explicitly restricts Section 7 protected activities. If the rule does not explicitly restrict protected activities, it will only violate Section 8(a)(1) upon a showing that: (1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights.

Rules that are ambiguous as to their application to Section 7 activity, and contain no limiting language or context that would clarify to employees that the rule does not restrict Section 7 rights, are unlawful. See University Medical Center, 335 NLRB 1318, 1320-1322 (2001), enf. denied in pertinent part 335 F.3d 1079 (D.C. Cir. 2003). In contrast, rules that clarify and restrict their scope by including examples of clearly illegal or unprotected conduct, such that they would not reasonably be construed to cover protected activity, are not unlawful. See Tradesmen International, 338 NLRB 460, 460-462 (2002).

The Employer in this case operates retail stores nationwide. Its social media policy, set forth in a section of its handbook titled "Information Security," provides in relevant part:

> **Use technology appropriately**
>
> * * * * *
>
> **If you enjoy blogging or using online social networking sites such as Facebook and YouTube, (otherwise known as Consumer Generated Media, or CGM) please note that there are guidelines to follow if you plan to mention [Employer] or your employment with [Employer] in these online vehicles. . .**

- **Don't release confidential guest, team member or company information. . . .**

We found this section of the handbook to be unlawful. Its instruction that employees not "release confidential guest, team member or company information" would reasonably be interpreted as prohibiting employees from discussing and disclosing information regarding their own conditions of employment, as well as the conditions of employment of employees other than themselves--activities that are clearly protected by Section 7. The Board has long recognized that employees have a right to discuss wages and conditions of employment with third parties as well as each other and that rules prohibiting the communication of confidential information without exempting Section 7 activity inhibit this right because employees would reasonably interpret such prohibitions to include information concerning terms and conditions of employment. See, e.g., Cintas Corp., 344 NLRB 943, 943 (2005), enfd. 482 F.3d 463 (D.C. Cir. 2007).

The next section of the handbook we addressed provides as follows:

Communicating confidential information

You also need to protect confidential information when you communicate it. Here are some examples of rules that you need to follow:

- **Make sure someone needs to know. You should never share confidential information with another team member unless they have a need to know the information to do their job. If you need to share confidential information with someone outside the company, confirm there is proper authorization to do so. If you are unsure, talk to your supervisor.**
- **Develop a healthy suspicion. Don't let anyone trick you into disclosing confidential information. Be suspicious if asked to ignore identification procedures.**
- **Watch what you say. Don't have conversations regarding confidential information in the Breakroom or in any other open area. Never discuss confidential information at home or in public areas.**

Unauthorized access to confidential information: If you believe there may have been unauthorized access to confidential information or that confidential information may have been misused, it is your responsibility to report that information. . . .

We're serious about the appropriate use, storage and communication of confidential information. A violation of [Employer] policies regarding confidential

information will result in corrective action, up to and including termination. You also may be subject to legal action, including criminal prosecution. The company also reserves the right to take any other action it believes is appropriate.

We found some of this section to be unlawful. Initially, we decided that the provisions instructing employees not to share confidential information with co-workers unless they need the information to do their job, and not to have discussions regarding confidential information in the breakroom, at home, or in open areas and public places are overbroad. Employees would construe these provisions as prohibiting them from discussing information regarding their terms and conditions of employment. Indeed, the rules explicitly prohibit employees from having such discussions in the breakroom, at home, or in public places--virtually everywhere such discussions are most likely to occur.

We also found unlawful the provisions that threaten employees with discharge or criminal prosecution for failing to report unauthorized access to or misuse of confidential information. Those provisions would be construed as requiring employees to report a breach of the rules governing the communication of confidential information set forth above. Since we found those rules unlawful, the reporting requirement is likewise unlawful.

We did not, however, find unlawful that portion of the handbook section that admonishes employees to "[d]evelop a healthy suspicion[,]" cautions against being tricked into disclosing confidential information, and urges employees to "[b]e suspicious if asked to ignore identification procedures." Although this section also refers to confidential information, it merely advises employees to be cautious about unwittingly divulging such information and does not proscribe any particular communications. Further, when the Employer rescinds the offending "confidentiality" provisions, this section would not reasonably be construed to apply to Section 7 activities, particularly since it specifically ties confidential information to "identification procedures." [Target Corp., Case 29-CA-030713]

Several Policy Provisions Are Overbroad, Including Those on 'Non-Public Information' and 'Friending Co-Workers'

In this case, we again found that certain portions of the Employer's policy governing the use of social media would reasonably be construed to chill the exercise of Section 7 rights in violation of the Act.

The Employer--a motor vehicle manufacturer--maintains a social media policy that includes the following:

> **USE GOOD JUDGMENT ABOUT WHAT YOU SHARE AND HOW YOU SHARE**
>
> **If you engage in a discussion related to [Employer], in addition to disclosing that you work for [Employer] and that your views are personal, you must also be sure that your posts are completely accurate and not misleading and that they do not reveal non-public company information on any public site. If you are in doubt, review the [Employer's media] site. If you are still in doubt, don't post. Non-public information includes:**
>
> - **Any topic related to the financial performance of the company;**
> - **Information directly or indirectly related to the safety performance of [Employer] systems or components for vehicles;**
> - **[Employer] Secret, Confidential or Attorney-Client Privileged information;**
> - **Information that has not already been disclosed by authorized persons in a public forum; and**
> - **Personal information about another [Employer] employee, such as his or her medical condition, performance, compensation or status in the company.**
>
> **When in doubt about whether the information you are considering sharing falls into one of the above categories, DO NOT POST. Check with [Employer] Communications or [Employer] Legal to see if it's a good idea. Failure to stay within these guidelines may lead to disciplinary action.**
>
> - **Respect proprietary information and content, confidentiality, and the brand, trademark and copyright rights of others. Always cite, and obtain permission, when quoting someone else. Make sure that any photos, music, video or other content you are sharing is legally sharable or that you have the owner's permission. If you are unsure, you should not use.**
> - **Get permission before posting photos, video, quotes or personal information of anyone other than you online.**
> - **Do not incorporate [Employer] logos, trademarks or other assets in your posts.**

We found various provisions in the above section to be unlawful. Initially, employees are instructed to be sure that their posts are "completely accurate and not misleading and that they do not reveal non-public information on any public site." The term "completely accurate and not misleading" is overbroad because it would reasonably be interpreted to apply to discussions about, or criticism of,

the Employer's labor policies and its treatment of employees that would be protected by the Act so long as they are not maliciously false. Moreover, the policy does not provide any guidance as to the meaning of this term by specific examples or limit the term in any way that would exclude Section 7 activity.

We further found unlawful the portion of this provision that instructs employees not to "reveal non- public company information on any public site" and then explains that non-public information encompasses "[a]ny topic related to the financial performance of the company"; "[i]nformation that has not already been disclosed by authorized persons in a public forum"; and "[p]ersonal information about another [Employer] employee, such as . . . performance, compensation or status in the company." Because this explanation specifically encompasses topics related to Section 7 activities, employees would reasonably construe the policy as precluding them from discussing terms and conditions of employment among themselves or with non-employees.

The section of the policy that cautions employees that "[w]hen in doubt about whether the information you are considering sharing falls into one of the [prohibited] categories, DO NOT POST. Check with [Employer] Communications or [Employer] Legal to see if it's a good idea[,]" is also unlawful. The Board has long held that any rule that requires employees to secure permission from an employer as a precondition to engaging in Section 7 activities violates the Act. See Brunswick Corp.,282 NLRB 794, 794-795 (1987).

The Employer's policy also unlawfully prohibits employees from posting photos, music, videos, and the quotes and personal information of others without obtaining the owner's permission and ensuring that the content can be legally shared, and from using the Employer's logos and trademarks. Thus, in the absence of any further explanation, employees would reasonably interpret these provisions as proscribing the use of photos and videos of employees engaging in Section 7 activities, including photos of picket signs containing the Employer's logo. Although the Employer has a proprietary interest in its trademarks, including its logo if trademarked, we found that employees' non-commercial use of the Employer's logo or trademarks while engaging in Section 7 activities would not infringe on that interest.

We found lawful, however, this section's bulleted prohibitions on discussing information related to the "safety performance of [Employer] systems or components for vehicles" and "Secret, Confidential or Attorney-Client Privileged information." Neither of these provisions refers to employees, and employees would reasonably read the safety

provision as applying to the safety performance of the Employer's automobile systems and components, not to the safety of the workplace. The provision addressing secret, confidential, or attorney-client privileged information is clearly intended to protect the Employer's legitimate interest in safeguarding its confidential proprietary and privileged information.

We also looked at the following provisions:

> **TREAT EVERYONE WITH RESPECT**
> **Offensive, demeaning, abusive or inappropriate remarks are as out of place online as they are offline, even if they are unintentional. We expect you to abide by the same standards of behavior both in the workplace and in your social media communications.**
>
> **OTHER [EMPLOYER] POLICIES THAT APPLY**
> **Think carefully about 'friending' co-workers . . . on external social media sites. Communications with co-workers on such sites that would be inappropriate in the workplace are also inappropriate online, and what you say in your personal social media channels could become a concern in the workplace.**
>
> **[Employer], like other employers, is making internal social media tools available to share workplace information within [Employer]. All employees and representatives who use these social media tools must also adhere to the following:**
>
> - **Report any unusual or inappropriate internal social media activity to the system administrator.**
>
> **[Employer's] Social Media Policy will be administered in compliance with applicable laws and regulations (including Section 7 of the National Labor Relations Act).**

As to these provisions, we found unlawful the instruction that "[o]ffensive, demeaning, abusive or inappropriate remarks are as out of place online as they are offline." Like the provisions discussed above, this provision proscribes a broad spectrum of communications that would include protected criticisms of the Employer's labor policies or treatment of employees. Similarly, the instruction to be aware that "[c]ommunications with co-workers . . . that would be inappropriate in the workplace are also inappropriate online" does not specify which communications the Employer would deem inappropriate at work and, thus, is ambiguous as to its application to Section 7.

The provision of the Employer's social media policy instructing employees to "[t]hink carefully about

'friending' co-workers" is unlawfully overbroad because it would discourage communications among co-workers, and thus it necessarily interferes with Section 7 activity. Moreover, there is no limiting language clarifying for employees that it does not restrict Section 7 activity.

We also found unlawful the policy's instruction that employees "[r]eport any unusual or inappropriate internal social media activity." An employer violates the Act by encouraging employees to report to management the union activities of other employees. See generally Greenfield Die & Mfg. Corp., 327 NLRB 237, 238 (1998) and cases cited at n.6. Such statements are unlawful because they have the potential to discourage employees from engaging in protected activities. Here, the Employer's instruction would reasonably be construed by employees as applying to its social media policy. Because certain provisions of that policy are unlawful, as set forth above, the reporting requirement is also unlawful.

Finally, we concluded that the policy's "savings clause," under which the Employer's "Social Media Policy will be administered in compliance with applicable laws and regulations (including Section 7 of the National Labor Relations Act)," does not cure the ambiguities in the policy's overbroad rules. [General Motors, Case 07-CA-053570]

Guidelines on Privacy, Legal Matters, Online Tone, Prior Permission, and Resolving Concerns Are Overbroad

In this case, we again found that some of the Employer's social media guidelines were overly broad in violation of Section 8(a)(1)of the Act.

The Employer is an international health care services company that manages billing and other services for health care institutions. We addressed challenges to various provisions in its social media policy, as set out below.

> **Respect Privacy. If during the course of your work you create, receive or become aware of personal information about [Employer's] employees, contingent workers, customers, customers' patients, providers, business partners or third parties, don't disclose that information in any way via social media or other online activities. You may disclose personal information only to those authorized to receive it in accordance with [Employer's] Privacy policies.**

We found that the portion of the rule prohibiting disclosure of personal information about the Employer's employees and contingent workers is unlawful because, in the

absence of clarification, employees would reasonably construe it to include information about employee wages and their working conditions. We found, however, that the portion of the rule prohibiting employees from disclosing personal information only to those authorized to receive it is not, in these circumstances, unlawful. Although an employer cannot require employees to obtain supervisory approval prior to engaging in activity that is protected under the Act, the Employer's rule here would not prohibit protected disclosures once the Employer removes the unlawful restriction regarding personal information about employees and contingent workers.

> **Legal matters. Don't comment on any legal matters, including pending litigation or disputes.**

We found that the prohibition on employees' commenting on any legal matters is unlawful because it specifically restricts employees from discussing the protected subject of potential claims against the Employer.

> **Adopt a friendly tone when engaging online. Don't pick fights. Social media is about conversations. When engaging with others online, adopt a warm and friendly tone that will encourage others to respond to your postings and join your conversation. Remember to communicate in a professional tone. . . . This includes not only the obvious (no ethnic slurs, personal insults, obscenity, etc.) but also proper consideration of privacy and topics that may be considered objectionable or inflammatory—such as politics and religion. Don't make any comments about [Employer's] customers, suppliers or competitors that might be considered defamatory.**

We found this rule unlawful for several reasons. First, in warning employees not to "pick fights" and to avoid topics that might be considered objectionable or inflammatory--such as politics and religion, and reminding employees to communicate in a "professional tone," the overall thrust of this rule is to caution employees against online discussions that could become heated or controversial. Discussions about working conditions or unionism have the potential to become just as heated or controversial as discussions about politics and religion. Without further clarification of what is "objectionable or inflammatory," employees would reasonably construe this rule to prohibit robust but protected discussions about working conditions or unionism.

> **Respect all copyright and other intellectual property laws. For [Employer's] protection as well as your own, it is critical that you show proper respect for the laws governing copyright, fair use of copyrighted**

material owned by others, trademarks and other intellectual property, including [Employer's] own copyrights, trademarks and brands. Get permission before reusing others' content or images.

We found that most of this rule is not unlawful since it does not prohibit employees from using copyrighted material in their online communications, but merely urges employees to respect copyright and other intellectual property laws. However, the portion of the rule that requires employees to "[g]et permission before reusing others' content or images" is unlawful, as it would interfere with employees' protected right to take and post photos of, for instance, employees on a picket line, or employees working in unsafe conditions.

You are encouraged to resolve concerns about work by speaking with co-workers, supervisors, or managers. [Employer] believes that individuals are more likely to resolve concerns about work by speaking directly with co-workers, supervisors or other management-level personnel than by posting complaints on the Internet. [Employer] encourages employees and other contingent resources to consider using available internal resources, rather than social media or other online forums, to resolve these types of concerns.

We found that this rule encouraging employees "to resolve concerns about work by speaking with co-workers, supervisors, or managers" is unlawful. An employer may reasonably suggest that employees try to work out concerns over working conditions through internal procedures. However, by telling employees that they should use internal resources rather than airing their grievances online, we found that this rule would have the probable effect of precluding or inhibiting employees from the protected activity of seeking redress through alternative forums.

Use your best judgment and exercise personal responsibility. Take your responsibility as stewards of personal information to heart. Integrity, Accountability and Respect are core [Employer] values. As a company, [Employer] trusts—and expects—you to exercise personal responsibility whenever you participate in social media or other online activities. Remember that there can be consequences to your actions in the social media world—both internally, if your comments violate [Employer] policies, and with outside individuals and/or entities. If you're about to publish, respond or engage in something that makes you even the slightest bit uncomfortable, don't do it.

We concluded that this rule was not unlawful. We noted that this section is potentially problematic because its

reference to "consequences to your actions in the social media world" could be interpreted as a veiled threat to discourage online postings, which includes protected activities. However, this phrase is unlawful only insofar as it is an outgrowth of the unlawful rules themselves, i.e., the Employer is stating the potential consequences to employees of violating the unlawful rules. Thus, rescission of the offending rules discussed above will effectively remedy the coercive effect of the potentially threatening statement here.

Finally, we looked at the Employer's "savings clause":

> **National Labor Relations Act. This Policy will not be construed or applied in a manner that improperly interferes with employees' rights under the National Labor Relations Act.**

We found that this clause does not cure the otherwise unlawful provisions of the Employer's social media policy because employees would not understand from this disclaimer that protected activities are in fact permitted. [McKesson Corp., Case 06-CA-066504]

Provisions on Protecting Information and Expressing Opinions Are Too Broad, But Bullying Provision Is Lawful

In another case, we concluded that several portions of the Employer's social media policy are unlawfully overbroad, but that a prohibition on online harassment and bullying is lawful.

We first looked at the portion of the Employer's policy dealing with protection of company information:

> **Employees are prohibited from posting information regarding [Employer] on any social networking sites (including, but not limited to, Yahoo finance, Google finance, Facebook, Twitter, LinkedIn, MySpace, LifeJournal and YouTube), in any personal or group blog, or in any online bulletin boards, chat rooms, forum, or blogs (collectively, 'Personal Electronic Communications'), that could be deemed material non-public information or any information that is considered confidential or proprietary. Such information includes, but is not limited to, company performance, contracts, customer wins or losses, customer plans, maintenance, shutdowns, work stoppages, cost increases, customer news or business related travel plans or schedules. Employees should avoid harming the image and integrity of the company and any harassment, bullying, discrimination, or retaliation that would not be permissible in the workplace is not**

permissible between co-workers online, even if it is done after hours, from home and on home computers. . . .

We concluded that the rule prohibiting employees from posting information regarding the Employer that could be deemed "material non-public information" or "confidential or proprietary" is unlawful. The term "material non-public information," in the absence of clarification, is so vague that employees would reasonably construe it to include subjects that involve their working conditions. The terms "confidential or proprietary" are also overbroad. The Board has long recognized that the term "confidential information," without narrowing its scope so as to exclude Section 7 activity, would reasonably be interpreted to include information concerning terms and conditions of employment. See, e.g., University Medical Center, 335 NLRB at 1320, 1322. Here, moreover, the list of examples provided for "material non-public" and "confidential or proprietary" information confirms that they are to be interpreted in a manner that restricts employees' discussion about terms and conditions of employment. Thus, information about company performance, cost increases, and customer wins or losses has potential relevance in collective-bargaining negotiations regarding employees' wages and other benefits. Information about contracts, absent clarification, could include collective-bargaining agreements between the Union and the Employer. Information about shutdowns and work stoppages clearly involves employees' terms and conditions of employment.

We also found that the provision warning employees to "avoid harming the image and integrity of the company" is unlawfully overbroad because employees would reasonably construe it to prohibit protected criticism of the Employer's labor policies or treatment of employees.

We found lawful, however, the provision under which "harassment, bullying, discrimination, or retaliation that would not be permissible in the workplace is not permissible between co-workers online, even if it is done after hours, from home and on home computers." The Board has indicated that a rule's context provides the key to the "reasonableness" of a particular construction. For example, a rule proscribing "negative conversations" about managers that was contained in a list of policies regarding working conditions, with no further clarification or examples, was unlawful because of its potential chilling effect on protected activity. Claremont Resort and Spa, 344 NLRB 832, 836 (2005). On the other hand, a rule forbidding "statements which are slanderous or detrimental to the company" that appeared on a list of prohibited conduct including "sexual or racial harassment" and "sabotage" would not be reasonably understood to restrict Section 7 activity.

Tradesmen International, 338 NLRB at 462. Applying that reasoning here, we found that this provision would not reasonably be construed to apply to Section 7 activity because the rule contains a list of plainly egregious conduct, such as bullying and discrimination.

Next, we considered the portion of the Employer's policy governing employee workplace discussions through electronic communications:

> **Employees are permitted to express personal opinions regarding the workplace, work satisfaction or dissatisfaction, wages hours or work conditions with other [Employer] employees through Personal Electronic Communications, provided that access to such discussions is restricted to other [Employer] employees and not generally accessible to the public. . . .**
>
> **This policy is for the mutual protection of the company and our employees, and we respect an individual's rights to self-expression and concerted activity. This policy will not be interpreted or applied in a way that would interfere with the rights of employees to self organize, form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, or to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection or to refrain from engaging in such activities.**

We found that the provision prohibiting employees from expressing their personal opinions to the public regarding "the workplace, work satisfaction or dissatisfaction, wages hours or work conditions" is unlawful because it precludes employees from discussing and sharing terms and conditions of employment with non-employees. The Board has long recognized that "Section 7 protects employee communications to the public that are part of and related to an ongoing labor dispute." Valley Hospital Medical Center, 351 NLRB 1250, 1252 (2007), enfd. sub nom. Nevada Service Employees Union, Local 1107 v. NLRB, 358 F. App'x 783 (9th Cir. 2009).

We concluded that the Employer's "savings clause" does not cure the otherwise unlawful provisions. The Employer's policy specifically prohibits employees from posting information regarding Employer shutdowns and work stoppages, and from speaking publicly about "the workplace, work satisfaction or dissatisfaction, wages hours or work conditions." Thus, employees would reasonably conclude that the savings clause does not permit those activities. Moreover, the clause does not explain to a layperson what the right to engage in "concerted activity" entails. [Clearwater Paper Corp., Case 19-CA-064418]

Duty to Report 'Unsolicited' Electronic Communications Is Overbroad, But 'Unauthorized Postings' Provision Is Lawful

In this case, we found that the Employer unlawfully maintains an overly broad rule requiring employees who receive "unsolicited or inappropriate electronic communications" to report them. We found, however, that a prohibition on "unauthorized postings" is lawful.

The Employer is a nonprofit organization that provides HIV risk reduction and support services. The Employer's employee handbook contains an "Electronic Communications" policy, providing as follows:

> **Improper Use: Employees must use sound judgment in using [Employer's] electronic technologies. All use of electronic technologies must be consistent with all other [Employer] policies, including [Employer's] Professional Conduct policy. [Employer] management reserves the right to exercise its discretion in investigating and/or addressing potential, actual, or questionable abuse of its electronic technologies. Employees, who receive unsolicited or inappropriate electronic communications from persons within or outside [Employer], should contact the President or the President's designated agent.**

We concluded that the provision that requires employees to report any "unsolicited or inappropriate electronic communications" is overly broad under the second portion of the Lutheran Heritage test discussed above. We found that employees would reasonably interpret the rule to restrain the exercise of their Section 7 right to communicate with their fellow employees and third parties, such as a union, regarding terms and conditions of employment.

The policy also sets forth the following restriction on Internet postings:

> **No unauthorized postings: Users may not post anything on the Internet in the name of [Employer] or in a manner that could reasonably be attributed to [Employer] without prior written authorization from the President or the President's designated agent.**

We found that this provision is lawful. A rule that requires an employee to receive prior authorization before posting a message that is either in the Employer's name or could reasonably be attributed to the Employer cannot reasonably be construed to restrict employees' exercise of their Section 7 right to communicate about working conditions among themselves and with third parties. [Us Helping Us, Case 05-CA-036595]

Portions of Rules on Using Social Media and Contact with Media and Government Are Unlawful

In this case, we considered the Employer's rules governing employee use of social media, contact with the media, and contact with government agencies. We concluded that certain portions of these rules were unlawful as they would reasonably be interpreted to prohibit Section 7 activity.

Relevant portions of the Employer's rules are as follows:

> **[Employer] regards Social Media---blogs, forums, wikis, social and professional networks, virtual worlds, user-generated video or audio---as a form of communication and relationship among individuals. When the company wishes to communicate publicly---whether to the marketplace or to the general public---it has a well-established means to do so. Only those officially designated by [Employer] have the authorization to speak on behalf of the company through such media.**
>
> **We recognize the increasing prevalence of Social Media in everyone's daily lives. Whether or not you choose to create or participate in them is your decision. You are accountable for any publication or posting if you identify yourself, or you are easily identifiable, as working for or representing [Employer].**
>
> **You need to be familiar with all [Employer] policies involving confidential or proprietary information or information found in this Employee Handbook and others available on Starbase. Any comments directly or indirectly relating to [Employer] must include the following disclaimer: 'The postings on this site are my own and do not represent [Employer's] positions, strategies or opinions.'**
>
> **You may not make disparaging or defamatory comments about [Employer], its employees, officers, directors, vendors, customers, partners, affiliates, or our, or their, products/services. Remember to use good judgment.**
>
> **Unless you are specifically authorized to do so, you may not:**
>
> - **Participate in these activities with [Employer] resources and/or on Company time; or**
> - **Represent any opinion or statement as the policy or view of the [Employer] or of any individual in their capacity as an employee or otherwise on behalf of [Employer].**

> **Should you have questions regarding what is appropriate conduct under this policy or other related policies, contact your Human Resources representative or the [Employer]Corporate Communications Department. . . .**

We concluded that several aspects of this social media policy are unlawful. First, the prohibition on making "disparaging or defamatory" comments is unlawful. Employees would reasonably construe this prohibition to apply to protected criticism of the Employer's labor policies or treatment of employees. Second, we concluded that the prohibition on participating in these activities on Company time is unlawfully overbroad because employees have the right to engage in Section 7 activities on the Employer's premises during non-work time and in non-work areas. See Republic Aviation Corp. v. NLRB, 324 U.S. 793, 803 n.10 (1945).

We did not find unlawful, however, the prohibition on representing "any opinion or statement as the policy or view of the [Employer] or of any individual in their capacity as an employee or otherwise on behalf of [Employer]." Employees would not reasonably construe this rule to prohibit them from speaking about their terms and conditions of employment. Instead, this rule is more reasonably construed to prohibit comments that are represented to be made by or on behalf of the Employer. Thus, an employee could not criticize the Employer or comment about his or her terms and conditions of employment while falsely representing that the Employer has made or is responsible for making the comments. Similarly, we concluded that the requirement that employees must expressly state that their postings are "my own and do not represent [Employer's] positions, strategies or opinions" is not unlawful. An employer has a legitimate need for a disclaimer to protect itself from unauthorized postings made to promote its product or services, and this requirement would not unduly burden employees in the exercise of their Section 7 right to discuss working conditions.

We also considered the Contact with Media portion of the Employer's rules, which provides:

> **The Corporate Communications Department is responsible for any disclosure of information to the media regarding [Employer] and its activities so that accurate, timely and consistent information is released after proper approval. Unless you receive prior authorization from the Corporate Communications Department to correspond with members of the media or press regarding [Employer] or its business activities, you must direct inquiries to the Corporate Communications Department. Similarly, you have the**

obligation to obtain the written authorization of the Corporate Communications Department before engaging in public communications regarding [Employer] of its business activities.

You may not engage in any of the following activities unless you have prior authorization from the Corporate Communications Department:

- **All public communication including, but not limited to, any contact with media and members of the press: print (for example newspapers or magazines), broadcast (for example television or radio) and their respective electronic versions and associated web sites. Certain blogs, forums and message boards are also considered media. If you have any questions about what is considered media, please contact the Corporate Communications Department.**
- **Any presentations, speeches or appearances, whether at conferences, seminars, panels or any public or private forums; company publications, advertising, video releases, photo releases, news releases, opinion articles and technical articles; any advertisements or any type of public communication regarding [Employer] by the Company's business partners or any third parties including consultants.**

If you have any questions about the Contact with Media Policy, please contact the [Employer] Corporate Communications Department . . . .

We concluded that this entire section is unlawfully overbroad. While an employer has a legitimate need to control the release of certain information regarding its business, this rule goes too far. Employees have a protected right to seek help from third parties regarding their working conditions. This would include going to the press, blogging, speaking at a union rally, etc. As noted above, Section 7 protects employee communications to the public that are part of and related to an ongoing labor dispute. An employer rule that prohibits any employee communications to the media or, like the policy at issue here, requires prior authorization for such communications, is therefore unlawfully overbroad.

Finally, we looked at the rules' provisions on contact with government agencies:

Phone calls or letters from government agencies may occasionally be received. The identity of the individual contacting you should be verified. Additionally, the communication may concern matters involving the corporate office. The General Counsel

must be notified immediately of any communication involving federal, state or local agencies that contact any employee concerning the Company and/or relating to matters outside the scope of normal job responsibilities.

If written correspondence is received, notify your manager immediately and forward the correspondence to the General Counsel by PDF or facsimile and promptly forward any original documents. The General Counsel, if deemed necessary, may investigate and respond accordingly. The correspondence should not be responded to unless directed by an officer of the Company or the General Counsel.

If phone contact is made:

- **Take the individual's name and telephone number, the name of the agency involved, as well as any other identifying information offered;**
- **Explain that all communications of this type are forwarded to the Company's General Counsel for a response;**
- **Provide the individual with the General Counsel's name and number . . . if requested, but do not engage in any further discussion. An employee cannot be required to provide information, and any response may be forthcoming after the General Counsel has reviewed the situation; and**
- **Immediately following the conversation, notify a supervisor who should promptly contact the General Counsel.**

We concluded that this rule is an unlawful prohibition on talking to government agencies, particularly the NLRB. The Employer could have a legitimate desire to control the message it communicates to government agencies and regulators. However, it may not do so to the extent that it restricts employees from their protected right to converse with Board agents or otherwise concertedly seek the help of government agencies regarding working conditions, or respond to inquiries from government agencies regarding the same. [DISH Network, Case 16-CA-066142]

Employer's Entire Revised Social Media Policy--With Examples of Prohibited Conduct--Is Lawful

In this case, we concluded that the Employer's entire revised social media policy, as attached in full, is lawful. We thus found it unnecessary to rule on the Employer's social media policy that was initially alleged to be unlawful.

As explained above, rules that are ambiguous as to their application to Section 7 activity and that contain no limiting language or context to clarify that the rules do not restrict Section 7 rights are unlawful. In contrast, rules that clarify and restrict their scope by including examples of clearly illegal or unprotected conduct, such that they could not reasonably be construed to cover protected activity, are not unlawful.

Applying these principles, we concluded that the Employer's revised social media policy is not ambiguous because it provides sufficient examples of prohibited conduct so that, in context, employees would not reasonably read the rules to prohibit Section 7 activity. For instance, the Employer's rule prohibits "inappropriate postings that may include discriminatory remarks, harassment and threats of violence or similar inappropriate or unlawful conduct." We found this rule lawful since it prohibits plainly egregious conduct, such as discrimination and threats of violence, and there is no evidence that the Employer has used the rule to discipline Section 7 activity.

Similarly, we found lawful the portion of the Employer's social media policy entitled "Be Respectful." In certain contexts, the rule's exhortation to be respectful and "fair and courteous" in the posting of comments, complaints, photographs, or videos, could be overly broad. The rule, however, provides sufficient examples of plainly egregious conduct so that employees would not reasonably construe the rule to prohibit Section 7 conduct. For instance, the rule counsels employees to avoid posts that "could be viewed as malicious, obscene, threatening or intimidating." It further explains that prohibited "harassment or bullying" would include "offensive posts meant to intentionally harm someone's reputation" or "posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy." The Employer has a legitimate basis to prohibit such workplace communications, and has done so without burdening protected communications about terms and conditions of employment.

We also found that the Employer's rule requiring employees to maintain the confidentiality of the Employer's trade secrets and private and confidential information is not unlawful. Employees have no protected right to disclose trade secrets. Moreover, the Employer's rule provides sufficient examples of prohibited disclosures (i.e., information regarding the development of systems, processes, products, know-how, technology, internal reports, procedures, or other internal business-related communications) for employees to understand that it does not reach protected communications about working conditions. [Walmart, Case 11-CA-067171]

Social Media Policy

Updated: May 4, 2012

At [Employer], we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media.

This policy applies to all associates who work for [Employer], or one of its subsidiary companies in the United States ([Employer]).

Managers and supervisors should use the supplemental Social Media Management Guidelines for additional guidance in administering the policy.

GUIDELINES

In the rapidly expanding world of electronic communication, *social media* can mean many things. *Social media* includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with [Employer], as well as any other form of electronic communication.

The same principles and guidelines found in [Employer] policies and three basic beliefs apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow associates or otherwise adversely affects members, customers, suppliers, people who work on behalf of [Employer] or [Employer's] legitimate business interests may result in disciplinary action up to and including termination.

Know and follow the rules

Carefully read these guidelines, the [Employer] Statement of Ethics Policy, the [Employer] Information Policy and the Discrimination & Harassment Prevention Policy, and ensure your postings are consistent with these policies. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

Be respectful

Always be fair and courteous to fellow associates, customers, members, suppliers or people who work on behalf of [Employer]. Also, keep in mind that you are more likely to resolved work-related complaints by speaking directly with your co-workers or by utilizing our Open Door Policy than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably

could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, members, associates or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy.

Be honest and accurate

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about [Employer], fellow associates, members, customers, suppliers, people working on behalf of [Employer] or competitors.

Post only appropriate and respectful content

- Maintain the confidentiality of [Employer] trade secrets and private or confidential information. Trades secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential communications.
- Respect financial disclosure laws. It is illegal to communicate or give a "tip" on inside information to others so that they may buy or sell stocks or securities. Such online conduct may also violate the Insider Trading Policy.
- Do not create a link from your blog, website or other social networking site to a [Employer] website without identifying yourself as a [Employer] associate.
- Express only your personal opinions. Never represent yourself as a spokesperson for [Employer]. If [Employer] is a subject of the content you are creating, be clear and open about the fact that you are an associate and make it clear that your views do not represent those of [Employer], fellow associates, members, customers, suppliers or people working on behalf of [Employer]. If you do publish a blog or post online related to the work you do or subjects associated with [Employer], make it clear that you are not speaking on behalf of [Employer]. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of [Employer]."

Using social media at work

Refrain from using social media while on work time or on equipment we provide, unless it is work-related as authorized by your manager or consistent with the Company Equipment Policy. Do not use [Employer] email addresses to register on social networks, blogs or other online tools utilized for personal use.

Retaliation is prohibited

[Employer] prohibits taking negative action against any associate for reporting a possible deviation from this policy or for cooperating in an investigation. Any associate who retaliates against another associate for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

Media contacts

Associates should not speak to the media on [Employer's] behalf without contacting the Corporate Affairs Department. All media inquiries should be directed to them.

For more information

If you have questions or need further guidance, please contact your HR representative.