Volume 5, Issue 6, November 2014

SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

THE BURTON AWARDS FOR THE PURSUIT OF PERFECTION
2011 BEST LAW FIRM NEWSLETTER

IN THIS ISSUE

To Click or Not to Click? Ninth Circuit Rejects Browsewrap Arbitration Clause
Page 2

"Operation Full Disclosure": FTC Warns Advertisers to Check the Fine Print
Page 3

New York Family Court Magistrate Allows Unprecedented Service of Process via Facebook; Will Others Follow?
Page 5

Breaking Old Ground: California Again Amends Data Security Breach Law
Page 5

Federal District Court Holds Facebook Fan Page Manager Doesn't Own "Likes"
Page 7

UK Financial Services Regulator Issues Draft Guidance on Social Media: Should We Favorite or Fail?
Page 8

EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

Patrick Bernhardt
John F. Delaney
Aramide O. Fields
Reed Freeman
Sherman Kahn
David McDowell
Susan McLean
Nathan D. Taylor

FOLLOW US

Morrison & Foerster's Socially Aware Blog

@MoFoSocMedia

MORRISON FOERSTER

In this issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media, we discuss an important Ninth Circuit decision refusing to enforce an arbitration clause in a website "terms of use" agreement; we examine "Operation Full Disclosure," the Federal Trade Commission's initiative to review fine print disclosures and other disclosures in connection with advertisements; we highlight a recent case allowing unprecedented service of process via Facebook; we take a look at California's recent data security breach law amendment, which may impose the country's first requirement to provide free identify theft protection services to consumers in connection with certain data security breaches; we explore a new court decision addressing ownership issues in connection with Facebook "likes"; and we review the UK Financial Conduct Authority's draft guidelines on social media.

All this—plus an infographic regarding mobile device and app use.

TO CLICK OR NOT TO CLICK? NINTH CIRCUIT REJECTS BROWSEWRAP ARBITRATION CLAUSE

By John Delaney and Sherman Kahn

In *Kevin Khoa Nguyen v. Barnes & Noble Inc.*, 2014 U.S. App. LEXIS 15868 (9th Cir. 2014), decided on August 18, 2014, the Ninth Circuit rejected an attempt to bind a consumer to an arbitration clause found in an online terms of use agreement not affirmatively "click accepted" by the consumer but readily accessible through a hyperlink at the bottom left of each page on the subject website.

The case arose from a "fire sale" by defendant Barnes & Noble of certain discontinued Hewlett Packard TouchPads. Plaintiff Nguyen had ordered two of the TouchPads, but received a notice from Barnes & Noble the following day that his order had been cancelled due to unexpectedly high demand. Nguyen sued Barnes & Noble in California Superior Court on behalf of himself and a putative class, arguing that he was forced to buy a more expensive tablet instead.

Barnes & Noble, after removing the suit to federal court, moved to compel arbitration under the Federal Arbitration Act, arguing that, by using the Barnes & Noble website, Nguyen had agreed to an arbitration clause contained in Barnes & Noble's Terms of Use. Nguyen responded that he could not be bound to the arbitration clause because he had no notice of and did not consent to the Terms of Use. Barnes & Noble countered that the placement of the Terms of Use hyperlink on its website had given Nguyen constructive notice of the arbitration clause.

The district court agreed with Nguyen, Barnes & Noble appealed, and the Ninth Circuit affirmed.

We have previously surveyed the law in this area here (regarding the *Nguyen* district court decision) and here (regarding other decisions involving online arbitration clauses). The Ninth Circuit's opinion in *Nguyen* is generally consistent with the existing caselaw, which suggests that, absent evidence of affirmative consent, courts are reluctant to find that parties—especially consumers—are bound by arbitration clauses contained in online terms of use agreements.

> The determination of the validity of the browsewrap contract depends on whether the user has actual or constructive knowledge of the website's terms and conditions.

In *Nguyen*, it was established that Barnes & Noble made available a hyperlink to its Terms of Use at the bottom left corner of each page on its website. Further, on each page of the website's online checkout process, Barnes & Noble presented, underlined and in green type, a hyperlink to its Terms of Use. However, it was apparently undisputed that Nguyen had neither clicked on the Terms of Use hyperlink nor actually read the Terms of Use.

To determine whether a valid arbitration clause exists, courts apply ordinary state law principles of contract formation. Interestingly, in *Nguyen*, the Ninth Circuit applied New York law as provided in the Barnes & Noble Terms of Use even though the question was whether such Terms of Use were a valid agreement in the first instance. The Ninth Circuit noted, however, that its analysis would be the same under California law as under New York law.

Applying New York law, the Ninth Circuit examined the law of "clickwrap" and "browsewrap" agreements and commented that "[t]he defining feature of browsewrap agreements is that the user can continue to use the website or other services without visiting the page hosting the browsewrap agreement or even knowing that such a web page exists." Thus, the Ninth Circuit observed, the determination of the validity of the browsewrap contract depends on whether the user has actual or constructive knowledge of the website's terms and conditions.

The Ninth Circuit noted that courts have consistently enforced browsewrap agreements where the user had actual notice of the agreement but pointed out that courts are more willing to enforce browsewrap agreements where the browsewrap agreement resembles a clickwrap agreement, i.e., where the user is required to affirmatively acknowledge the agreement in some way.

The Ninth Circuit further stated that where, as in the case of *Nguyen*, no evidence exists that the user had any knowledge of a browsewrap agreement, the validity of such agreement turns on whether the disclosure of the agreement on the website is sufficient to put a reasonably prudent user on notice of the terms and conditions of such agreement. This inquiry turns on the design and content of the website. Where the link to the terms of use is hidden at the bottom of the page or tucked away in obscure corners of the website, notice is not sufficient.

> The onus must be on website owners to put users on notice of the terms to which they wish to bind consumers.

MOBILE DEVICES & APPS BY THE NUMBERS

Mobile App Use

Mobile app use increased by **21%** last year.[1]

51% **of computer use time is now spent on mobile apps.**[2]

Smartphone & Tablet Use

60% of computer use time is now conducted via smartphones and tablets.[2]

96% **of millennials have browsed the web using a smartphone.**[3]

32% of millennials have used a smartphone to make purchases or reservations.[2]

Mobile Use of Social Media

24% of mobile time is spent on Facebook, making it the #1 mobile property.[2]

70% **of social networking activity is being generated via mobile.**[2]

SOURCES

1. http://info.localytics.com/blog/time-in-app-increases-by-21-across-all-apps
2. http://www.comscore.com/Insights/Blog/Major-Mobile-Milestones-in-May-Apps-Now-Drive-Half-of-All-Time-Spent-on-Digital
3. http://www.slideshare.net/RJIonline/2014-mmnc-charts-4
   (chart 4.3. Results based on a survey of 1,191 adults)

The Ninth Circuit's analysis in *Nguyen* relies heavily on the Second Circuit's decision in *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2d Cir. 2002), in which the Second Circuit had rejected an arbitration clause in a terms of use agreement for inadequate notice. The Ninth Circuit acknowledged that Barnes & Noble's placement of the link to its Terms of Use at the bottom left of every page and also close to the buttons a user must click to complete a transaction distinguished the case from *Specht*, in which the link at issue was on a submerged screen that could not be seen unless the user scrolled past the button that initiated the relevant transaction. However, the Ninth Circuit held that the proximity or conspicuousness of the hyperlink alone was not enough to give rise to constructive notice. Rather, the Ninth Circuit said, the onus must be on website owners to put users on notice of the terms to which they wish to bind consumers.

What then must a website owner do to provide the requisite notice? A clear manifestation of consent is the safest way to ensure enforceability—for example, by requiring the user to check an unchecked box before allowing the user to complete a transaction.

The Ninth Circuit also suggests in *Nguyen* that a clear textual notice on the website that continued use will act as a manifestation of the user's intent to be bound by the terms of use may also result in an effective agreement.

It also noted in a footnote that the standard may be higher where agreements are being enforced against consumers rather than against business entities.

In any event, *Nguyen* is a wake-up call for website operators for whom it is critical that an arbitration clause embedded in their website terms of use is enforceable; serious consideration needs to be given to how best to strengthen the enforceability of such clauses in the wake of the Ninth Circuit's decision.

More generally, *Nguyen* is a reminder for all website operators that those ubiquitous browsewrap terms of use—found on nearly every website, big and small, across the entire span of the Internet—have serious limitations as a tool for legally binding site visitors and mitigating risks.

"OPERATION FULL DISCLOSURE": FTC WARNS ADVERTISERS TO CHECK THE FINE PRINT

By David McDowell, Aramide O. Fields and Reed Freeman

The Federal Trade Commission (FTC) announced recently that it sent warning letters to more than 60 national advertisers

regarding the inadequacy of disclosures in their television and print ads. The letters are part of an initiative named "Operation Full Disclosure," which the FTC implemented to review fine print disclosures and other disclosures that it believed were difficult to read or easy for consumers to overlook, yet included critical information that consumers would need to avoid being misled.

WHAT DOES IT MEAN FOR A DISCLOSURE TO BE "CLEAR AND CONSPICUOUS"

Disclosures may be necessary to clarify a claim or to ensure that the full terms of an offer are adequately disclosed, in order to avoid a charge of deception by material omission. In FTC jurisprudence, disclosures must be "clear and conspicuous," and while they may *modify* claims in the text of an ad itself, they may not contradict any such claims. The most recent pronouncement on how to make effective disclosures (this one was focused on online disclosures, but the general principles are the same) was issued in March 2013. *The key is that if a disclosure is necessary to make an ad truthful and not misleading, it must be clear and conspicuous; otherwise, it is as though the disclosure was not made at all.*

Whether a disclosure is adequate to meet the "clear and conspicuous" test depends on a number of factors, the most important of which are:

- the placement of the disclosure in the advertisement and its proximity to the claim it is qualifying;
- the prominence of the disclosure;
- whether the disclosure is unavoidable;
- the extent to which items in other parts of the advertisement might distract attention from the disclosure;
- whether the disclosure needs to be repeated several times in order to be effectively communicated, or because consumers may enter the site at different locations or travel through the site on paths that cause them to miss the disclosure;
- whether disclosures in audio messages are presented in an adequate volume and cadence and visual disclosures appear for a sufficient duration; and
- whether the language of the disclosure is understandable to the intended audience.

Advertisers would be well-advised to review their ads and disclosures anew to make sure they comply with the FTC's standards for clear and conspicuous disclosures in both offline and online advertising.

NEXT STEPS: LAW ENFORCEMENT SWEEP?

In light of the FTC's recent warnings, advertisers would be well-advised to review their ads and disclosures anew to make sure they comply with the FTC's standards for clear and conspicuous disclosures in both offline and online advertising. We expect the FTC may well follow this group of warning letters with a series of enforcement actions, as it did in 1996 against a number of auto manufacturers for the mouse print in their leasing ads. The FTC followed up with Mazda in 1999, alleging that it failed to abide by the FTC's stipulated order on proper disclosures, settling for $5.25 million.

WHAT DID THE FTC HIGHLIGHT IN THE WARNING LETTERS?–MAKE SURE YOU GET THESE RIGHT!

Although the FTC has not disclosed which companies received the warning letters, it indicated that the 60-plus recipients include 20 of the largest advertisers in the country, a wide range of industries and types of products, and both English- and Spanish-language ads. FTC staff sought to identify a representative sample of advertisers that made inadequate disclosures and emphasized that advertisers who did not receive a letter should not assume that their ads are fine simply because they did not receive a warning letter.

Similarly, the FTC's focus on television and print ads does not mean that other forms of advertising get a pass; the FTC is equally concerned about disclosures that appear in other media, such as online and on mobile devices.

The FTC identified several types of inadequate disclosures in the television and print ads it reviewed. Examples of the inadequate disclosures include the following:

- quoting the price of a product or service without disclosing conditions for obtaining the price;
- failing to disclose an automatic billing feature;
- claiming that a product capability of an accessory was included without disclosing the need to first buy or own an additional product or service;
- claiming that a product was unique or superior in a product category without disclosing the advertiser's narrow definition of the category;
- making comparative claims without disclosing the basis of the advertiser's comparisons;
- promoting a "risk-free" or "worry-free" trial period without disclosing that consumers have to pay shipping costs; and
- making absolute or broad statements without explaining relevant exceptions or limitations.

CONCLUSION

In light of the FTC's recent warnings, advertisers would be well-advised to review their ads and disclosures anew to make sure they comply with the FTC's standards.

NEW YORK FAMILY COURT MAGISTRATE ALLOWS UNPRECEDENTED SERVICE OF PROCESS VIA FACEBOOK; WILL OTHERS FOLLOW?

By John Delaney

In a little-noticed decision, *Matter of Noel v. Maria*, Support Magistrate Gregory L. Gliedman—a Staten Island, New York family court official—recently permitted a father seeking to modify his child support payments *to serve process on the child's mother by sending her a digital copy of the summons and petition through her Facebook account*.

Magistrate Gliedman's decision struck us at *Socially Aware*—where we follow such developments closely—as a groundbreaking move. We are unaware of any published U.S. court opinion permitting a plaintiff to serve process on a domestic, U.S.-based defendant through a Facebook account.

As we addressed in a 2012 *Socially Aware* blog post, in *Fortunato v. Chase Bank*, a federal district court in Manhattan held that Chase Bank could not rely on Facebook to serve a third-party defendant.

While the same federal district court subsequently allowed the FTC to serve defendants through Facebook in *FTC v. PCCare247*, the service at issue in that case concerned documents other than the summons and complaint, and the defendants were two India-based entities and three India-based individuals who had already appeared through counsel and shown themselves to be on notice of the lawsuit.

Other cases authorizing service via social media have been similarly limited in scope. For example, in *WhosHere v. Orun*, the U.S. District Court for the Eastern District of Virginia allowed service via social media on a defendant who allegedly resided in Turkey. In *Mpafe v. Mpafe*, a Minnesota family court authorized the service of divorce proceedings on a defendant by "Facebook, Myspace or any other social networking site" where the defendant was believed to have left the country.

We are unaware of any published U.S. court opinion permitting a plaintiff to serve process on a domestic, U.S.-based defendant through a Facebook account.

Further, the court in *FTC v. PCCare247* permitted Facebook service only as a backstop to service by regular email, and specified that Facebook service alone might not satisfy due process because—as the court understood it—"anyone can make a Facebook profile using real, fake, or incomplete information, and thus, there is no way for the Court to confirm whether the [party] the investigator found is in fact the third-party Defendant to be served."

Of course, Facebook has been well known for requiring use of one's real name in opening a Facebook account. And although Facebook recently modified its real-name policy to accommodate stage names, Facebook remains strongly opposed to fake accounts. That being said, Facebook has acknowledged that many unauthorized accounts exist on its platform.

Moreover, with more than 1.5 billion users, it's not uncommon for people sharing the same or similar names to be mistaken for one another on Facebook; if you can accidentally send a friend request to a stranger who happens to share a name with a childhood classmate, could you end up serving process on the wrong person via a Facebook message?

And although a 2013 study revealed that smartphone users access their Facebook accounts an average of 14 times a day (!), might there be people out there who have a Facebook account but rarely if ever check it? Of course, this particular concern may be overcome by showing that a defendant is actively using his or her Facebook account; indeed, in *Matter of Noel v. Maria*, the father presented evidence that the mother had recently "liked" photos posted to another Facebook page, indicating that the mother was in fact an active Facebook user.

In any event, Magistrate Gliedman's decision represents a significant milestone, and deserves greater attention and discussion. As Facebook and other social media practices become ever more deeply integrated into our lives, expect to see other judges and magistrates exploring—and perhaps even expanding—the circumstances under which service of process via a social media channel is deemed appropriate.

BREAKING OLD GROUND: CALIFORNIA AGAIN AMENDS DATA SECURITY BREACH LAW

By Nathan D. Taylor and Patrick Bernhardt

Not to be outdone by Florida, California has yet again amended its data security breach law and again in groundbreaking (yet confusing) fashion. On September 30, 2014, California Governor Brown signed into law a bill ("AB 1710") that appears to impose the country's first requirement to provide free identity theft protection services to consumers

in connection with certain data security breaches. The law also amends the state's personal information safeguards law and Social Security number (SSN) law. The amendments will become effective on January 1, 2015.

FREE IDENTITY THEFT PROTECTION SERVICES REQUIRED FOR CERTAIN BREACHES

Most significantly, AB 1710 appears to amend the California breach law to require that a company offer a California resident "appropriate identity theft prevention and mitigation" services, at no cost, if a breach involves that individual's name and SSN, driver's license number or California identification card number. Specifically, AB 1710 provides, in pertinent part, that if a company providing notice of such a breach was "the source of the breach":

> "an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached."

The drafting of this requirement is far from clear and open to multiple readings. In particular, the use of the phrase "if any" can be read in multiple ways. For example, the phrase "if any" can be read to modify the phrase "appropriate identity theft prevention and mitigation services." Under this reading, the law would impose an obligation to provide free identity theft protection services if any such services are appropriate. The phrase "if any," however, could be read to modify the "offer" itself. Under this alternate reading, the law would provide that if a company intends to offer identity theft protection services, those services must be at no cost to the consumer. It is difficult to know how the California Attorney General (AG) or California courts will interpret this ambiguity. One thing is clear: until the AG or courts opine, the standard will remain unclear.

The drafting of the requirement also is not clear in other ways. For example, the statute does not specify what type of services would qualify as "appropriate identity theft prevention and mitigation services." Would a credit monitoring product alone be sufficient to meet the requirement? Or would the law require something in addition to credit monitoring, such as an identity theft insurance element?

The new law appears to impose the country's first requirement to provide free identity theft protection services to consumers in connection with certain data security breaches.

Nonetheless, state AGs historically have encouraged companies to provide free credit monitoring to consumers following breaches. In addition, even though not legally required, free credit monitoring has become a common practice, particularly for breaches involving SSNs and also increasingly for high-profile breaches. Nonetheless, California appears to be the first state to legally require that companies offer some type of a free identity theft protection service for certain breaches.

AB 1710 is particularly notable in its approach. First, the offer of free identity theft protection services will only be required for breaches involving SSNs, driver's licenses or California identification card numbers. In this regard, an offer of free identity theft protection services will not be required for breaches involving other types of covered personal information, such as payment card information or usernames and passwords. This approach endorses a position that many companies have long held—that credit monitoring is appropriate only when the breach creates an actual risk of new account identity theft (as opposed to fraud on existing accounts). In addition, the offer of free identity theft protection services will only be required for a period of one year (as opposed to, for example, two years). The length of the offer of free credit monitoring has always been an issue of debate, and California has now endorsed a position that a one-year offer is sufficient.

SERVICE PROVIDERS DIRECTLY SUBJECT TO SAFEGUARDS REQUIREMENTS

AB 1710 also amends the California personal information safeguards law to impose the state's safeguards obligations directly on entities who "maintain" information, even if they do not own that information. The state's safeguards standard historically required companies that "own or license" covered personal information about California residents to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" in order to protect the personal information from unauthorized activity. The existing standard did not apply directly to third parties, such as service providers, that maintain information, but do not own it. Instead, the existing standard required that owners of personal information contractually require nonaffiliated third parties to whom they would disclose such information to take steps to protect the information.

AB 1710, however, specifically amends the safeguards law to impose its reasonable security procedures and practices standard directly on entities that "maintain" covered personal information, even if they do not "own or license" the data. Moreover, AB 1710 eliminates the requirement to pass-

through security obligations by contract to certain third parties. Specifically, AB 1710 provides that the third-party contract requirement does not apply to a company that provides covered personal information to a third party that will now be directly subject to the safeguards standard (i.e., a third party that "maintains" covered personal information). As a result, the third-party contract requirement would appear to apply only when a company discloses covered personal information to a nonaffiliated third party that will handle such data, but not "maintain" it.

NEW PROHIBITION ON SALE OF SSNS

Finally, AB 1710 amends the California SSN law to prohibit any person from selling, advertising for sale or offering to sell an individual's SSN. Moreover, AB 1710 specifically provides that the "[r]elease of an individual's [SSN] for marketing purposes is not permitted." This new prohibition on the sale of SSNs, however, will not apply: (1) if the disclosure of the SSN is incidental to a larger transaction and is necessary to identify the individual in order to accomplish a legitimate business purpose; or (2) for a purpose specifically authorized or allowed by federal or state law. Although AB 1710's limitation on the sale of SSNs is unique among the many state SSN laws, other state SSN laws do include similar prohibitions, such as the Alaska, Minnesota, North Carolina, South Carolina and Vermont laws.

PRACTICAL IMPLICATIONS FOR BUSINESSES

The California requirement regarding free identity theft protection services for certain breaches adds yet another layer of complexity for a company that suffers a breach. Companies should be prepared to make difficult decisions regarding how to implement the new requirement. For example, companies should consider the following:

- Until further guidance is provided by the AG or the courts, how will your company interpret the language of the requirement? For example, will your company take the position that AB 1710 does not actually impose a requirement to offer free identity theft protection services?
- What type of "appropriate identity theft prevention and mitigation" services will your company offer when it believes such an offer is required?
- In the event of a breach involving information regarding residents of multiple states, including California, will your company extend an offer of identity theft protection services to residents of states other than California?
- Will your company offer identity theft protection services in connection with breaches involving personal information other than SSN, driver's license number or California identification card number?
- When your company offers free identity theft protection services, will it provide the offer only for one year? Are there circumstances in which your company will extend an offer for a longer period?

Companies should be prepared to make difficult decisions regarding how to implement the new requirement.

As has been historically true, other states may follow California's lead. As a result, it will be important to monitor state legislative developments, and if a state imposes a similar requirement, determine if it follows a risk-based approach similar to AB 1710.

In addition, companies that provide services to others that involve maintaining personal information relating to California residents that is maintained but not owned should be aware that they will be directly subject to the requirements of the California safeguards law. Before AB 1710's new requirements become effective, such companies should take a fresh look at their security procedures and practices and consider whether they are appropriate and would comply with the California safeguards requirement.

FEDERAL DISTRICT COURT HOLDS FACEBOOK FAN PAGE MANAGER DOESN'T OWN "LIKES"

By John Delaney

A federal district court broke new social media law ground in August 2014 when it held in favor of the cable network Black Entertainment Television (BET) in a suit brought by the founder of an unofficial Facebook fan page for one of the network's television shows. In holding that BET acted lawfully when it asked Facebook to transfer the fan-created page's "likes" to a BET-sponsored page, the U.S. District Court for the Southern District of Florida established important precedent: The only individual who can possibly claim to own a "like" on a Facebook page is the individual user responsible for it.

BACKGROUND

Insurance agent Stacey Mattocks was so devoted to the television series *The Game* that she created an unofficial Facebook fan page for the show in 2008. By the time BET acquired the rights to *The Game* from the CW Network in 2009, Mattocks' fan page had garnered a huge following, and BET—reportedly having failed to attract similar support for the show's official fan page—wanted to capitalize on the social media audience that Mattocks had amassed.

> The only individual who can possibly claim to own a "like" on a Facebook page is the individual user responsible for it.

Thus began a series of negotiations between Mattocks and BET, with Mattocks at one point managing the page for the Viacom-owned cable channel for $30 an hour. During Mattocks' tenure in that part-time position, BET provided her with exclusive content to post on the Facebook page and began displaying its trademark and logos on it. The page's following grew from two million to more than six million fans.

At this point, in early 2011, Mattocks and BET entered into a letter agreement granting BET administrative access to the Facebook page and the right to post content on it in exchange for the network's promise not to change Mattocks' administrative rights to the page. But Mattocks broke the agreement in 2012 when, after refusing a reported $85,000 annual salary offer from BET, she cut off the network's control of the Facebook page and informed BET that she would maintain that restriction until the parties reached "an amicable and mutually beneficial resolution" concerning her employment.

BET reacted to being cut off by asking Facebook to "migrate" the page's fans to a BET-sponsored page. After determining that the BET-sponsored page officially represented *The Game*'s brand owner, Facebook complied. Twitter also complied with BET's separate request to disable *The Game* Twitter account that Mattocks maintained.

Mattocks filed suit in the U.S. District Court for the Southern District of Florida, alleging that BET tortiously interfered with Mattocks' contractual relationships with Facebook and Twitter; breached its letter agreement with Mattocks; breached a duty of good faith and fair dealing with Mattocks; and converted a business interest that Mattocks had in the page. In late August 2014, the court held that BET was entitled to summary judgment on all of Mattocks' claims.

THE DISMISSAL OF THE CONVERSION CLAIM

In his opinion, Judge James Cohn set out the case's most significant holding—that Mattocks couldn't establish a property interest in the "likes" on the Facebook page that she maintained for *The Game*—in the context of dismissing Mattocks' conversion claim. To prove a conversion claim under Florida law, Judge Cohn stated that "a plaintiff must offer facts sufficient to show ownership of the subject property." Mattocks couldn't establish that she owns a property interest in the "likes" on *The Game*'s Facebook page, Judge Cohn held, because of "the tenuous relationship between 'likes' on a Facebook page and the creator of the page," as is evidenced by the fact that a Facebook user always maintains the ability to revoke a "like" by clicking an "unlike" button.

> Companies need to have appropriate agreements in place with their employees and contractors who manage social media accounts for the companies' brands.

The court further opined that—based on a case holding that a public employee's "like" of a political-campaign page constitutes a protected form of free speech—"if anyone can be deemed to own the 'likes' on a page, it is the individual users responsible for them."

THE OPINION'S IMPACT ON BUSINESSES

The *Mattocks v. Black Entm't* case highlights the need for a company to have appropriate agreements in place with its employees and contractors who manage social media accounts for the company's brands.

Such agreements ideally should set out the company's ownership of the applicable social media accounts (although remember to review the terms of use for the relevant social media platforms to ensure consistency with respect to account ownership status); ensure account passwords are controlled by the company; and address the consequences of the employee's or consultant's possible termination.

Regarding account passwords, be wary of vesting full administrative access to a company social media account in a single employee; by providing for shared administrative access, a company increases the likelihood of maintaining access to such an account even if one of the company's social media managers is terminated. And, of course, a company should change its account passwords after ending its relationship with any employee or contractor who had been provided access to such passwords. (For other risk-reduction tips on this subject, please see our earlier article, "Ownership of Business-Related Social Media Accounts," located here.)

UK FINANCIAL SERVICES REGULATOR ISSUES DRAFT GUIDANCE ON SOCIAL MEDIA: SHOULD WE FAVORITE OR FAIL?

By Susan McLean

On August 6, 2014, the United Kingdom's financial services regulator, the Financial Conduct Authority (FCA), issued long-awaited draft guidance on the use of

social media in financial promotions by regulated financial institutions.

But if financial services firms operating in the UK were hoping that this guidance would provide them with a clear framework to help jump-start their social media strategies, they will be disappointed. For one thing, the guidance is focused on financial promotions, so firms will need to continue to evaluate all of their social media activities carefully against existing FCA rules.

The proposed guidance—"GC14/6 Social media and customer communications: The FCA's supervisory approach to financial promotions in social media" ("Guidance")—is open for consultation until November 6, 2014. The FCA intends to continue discussions with the financial services sector during the consultation period. It has also set up the hashtag #smfca for those wishing to discuss the Guidance on Twitter.

GUIDANCE

As outlined in our previous alert "Behind the Curve – Are Legal & Regulatory Concerns Preventing UK Financial Service Companies from Fully Harnessing Social Media?", until now the UK financial services regulator has offered very limited guidance on the use of social media. The FSA (the FCA's predecessor) issued in June 2010 a two-page, high-level guidance paper on financial promotions using new media. Compare this with the U.S. where various items of regulatory guidance (see our previous Guide to Social Media and the Securities Laws) on the use of social media, including from FINRA, FFIEC, and SEC, have been published.

This lack of regulatory clarity in the UK has been seen by some UK-based financial institutions as a deterrent from fully harnessing the benefits of social media, as highlighted at a recent Social Media Leadership Forum event.

In the new draft Guidance, the FCA acknowledges that social media can be a particularly powerful channel of communication, and is increasingly becoming the preferred media for customer communications and financial promotions. The FCA states that it does not want to prevent social media use, however, it acknowledges that forms of digital media often have character, space, and/or time limitations, which can constrain their use. It appreciates that, in some circumstances, firms may perceive difficulties in complying with the FCA's rules when using digital media. Accordingly, the Guidance is intended to clarify and confirm the FCA's approach to the supervision of financial promotions in social media.

The FCA's objectives include promoting effective competition in the interests of consumers, as well as consumer protection. The FCA accepts that digital media can allow new and smaller firms to have a presence in the marketplace, and may also allow firms to reach a wider audience. In principle, this can make it easier for consumers to switch providers and enhance competition. The FCA therefore sees significant potential benefits from the use of digital media by firms, as long as this is responsible and customer-focused.

The overarching principle for all communications with consumers is that they must be 'fair, clear and not misleading.'

The FCA repeats the position that it took in previous guidance and in all public statements made previously on the topic of social media (i.e., that its rules are intended to be media-neutral). The overarching principle for all communications with consumers is that they must be "fair, clear and not misleading."

The key recommendations included in the Guidance are as follows:

- Any form of communication made by a firm is capable of being a financial promotion; the key is whether it includes an invitation to engage in financial activity.
- Each communication must be considered individually and comply with the relevant rules.
- Some communications, including advertisements, will not include an invitation to engage in financial activity—for example, communications solely relating to the firm's community work, etc.
- Only financial promotions made in the course of business will be caught by the FCA rules. The definition laid down in the rules effectively requires a commercial interest on the part of the firm. The FCA provides a couple of examples to illustrate the issue:
  - If a company is already operating, it will be acting "in the course of business" when seeking to generate additional capital. If, however, the company has not yet been formed, and the proposed founders approach friends and family to obtain start-up capital, they will not generally be acting "in the course of business"; and
  - Where a personal social media account is used by someone associated with a business, say the CEO, for example, that business and individual should take care to distinguish clearly personal communications from those that are, or are likely to be understood to be, made in the course of that business.
- All financial promotions made via digital media must be clearly identified as such. If using Twitter, the FCA suggests including #ad in the tweet.
- Firms must identify risks, as well as benefits, and comply with applicable past performance rules.

- Risk warnings must be suitably prominent. If a risk warning is set out in too small a font size and/or lost in surrounding text, the promotion will not be compliant. Of course, social media often poses particular challenges because of space or character limitations. The FCA has suggested that one solution is to insert images (such as infographics into tweets)—as long as the image itself is compliant.
- The FCA acknowledges that the functionality which allows a Twitter image to be permanently visible may be switched off so that the image appears simply as a link. Accordingly, any risk warning or other information required by the rules cannot appear solely in the image.
- It may be possible to signpost a product or service with a link to more comprehensive information, provided that the signpost remains compliant in itself.
- Firms may be able to advertise through image advertising, which is less likely to cause compliance issues. An image advertisement (i.e., an advert that only includes the name of the firm, a logo or other image associated with the firm, contact point, and a reference to types of regulated activities provided by the firm or its fees or commissions) may be exempt from financial promotion rules, but will still need to be fair, clear, and not misleading.
- All communications must be fair, clear, and not misleading, even if the communication ends up in front of a non-intended recipient (e.g., due to a re-tweet, etc.). One way of managing this risk is to use software that enables advertisers to target particular groups very precisely.
- Where a recipient shares or forwards (e.g., re-tweets) a firm's communication, responsibility for that communication lies with the communicator so the firm would not be responsible (although the original communication would obviously still need to be compliant). If, however, a firm re-tweets a customer's tweet (e.g., one praising its customer service), the firm would be responsible even if the firm did not create the tweet.
- For the purpose of FCA rules, a tweet is not a real-time communication because it creates a record, is directed at multiple recipients, and doesn't require immediate response.
- Being a follower of a regulated firm on Twitter or having "liked" its Facebook page does not constitute an "existing client relationship" or "express request" for a communication under applicable rules. Issuing a financial promotion to such an individual would therefore be considered unsolicited.
- Firms need to put in place adequate systems for signing off digital media communications. Sign-off should be by a person of appropriate competence and seniority within the organization. The FCA doesn't address how this is achieved when social media activities themselves are outsourced.

OTHER ISSUES

The draft Guidance focuses on financial promotions, but firms are likely to have to consider other regulatory issues in the context of a social media strategy. For example, in terms of complaints-handling, it may be challenging for firms to identify when complaints are being made via social media and whether their complaints-handling procedures capture such complaints. In addition, if a firm outsources any critical activities as part of its social media strategy, it will need to take account of applicable outsourcing rules and guidance.

There is also a whole host of general legal issues arising from the use of social media that firms will need to consider, for example, in terms of:

- market abuse rules;
- employees' and agents' use of social media—both external platforms and internal communication/collaboration platforms;
- use of social media in recruitment;
- data privacy and security;
- crisis management and damage to reputation;
- protection and infringement of intellectual property rights;
- general advertising and marketing rules (e.g., the CAP Code);
- consumer protection/unfair terms and trading rules;
- user generated/third-party content; and
- insurance.

These issues are not covered in the draft Guidance.

CONCLUSION

The Guidance does not introduce any major surprises. The FCA had warned that the Guidance was not going to be prescriptive, and it isn't. By and large, it follows very closely existing guidance relating to financial promotions, and includes some pretty clear-cut examples of compliant and non-compliant communications.

In order to give firms further clarity in respect of their social media compliance, there are certain areas where the FCA could consider widening the scope of its Guidance improvements. For example:

- the Guidance appears to envisage a traditional form of promotion (albeit via digital media) which involves a firm simply publishing advertisements. Of course, social media is about more than one-way communication. Genuine interactive engagement is what consumers are looking for and is the key to the most successful social media strategy. Accordingly, it would be helpful for the FCA to include a few more

nuanced scenarios in its Guidance, such as where a firm's employee has a dialogue with a customer or potential customer via social media;

- as firms are increasingly using social media for customer services and complaints, it would be helpful to provide some illustrations of compliance in this area; and
- the FCA has communications with consumers very much in mind, but we know that firms in the Business-to-Business sector are increasingly using social media in their business. Accordingly, it would be helpful for the FCA to consider including some B2B-specific scenarios in the final Guidance;

So, overall, the draft Guidance is not a #fail, and is a step in the right direction, but #smfca is unlikely to be trending any time soon.

In the meantime, firms may just have to take a deep breath and take the plunge. After all, social media is just another way of communicating with customers. Firms need to exercise the same common sense, judgment, and risk-balancing that they use with other types of media. As social media is increasingly the way that consumers want to communicate, staying out of the game is no longer an option.

If you wish to receive a free subscription to our Socially Aware newsletter, please send a request via email to **sociallyaware@mofo.com**. We also cover social media-related business and legal developments on our Socially Aware blog, located at **www.sociallyawareblog.com**.

For breaking news related to social media law, follow us on Twitter **@MoFoSocMedia**. To review earlier issues of Socially Aware, visit us at **www.mofo.com/sociallyaware**.