

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

There Has Been a Data Security Breach: But is Notice Required?

By [Ronald I. Raether, Jr.](#)

It is Friday afternoon. You are looking forward to a relaxing weekend, spending time with your friends and finally getting around to that list of activities that you have not had time for lately. Just a few more emails, and it is off to dinner at your favorite restaurant. At least that was the plan until just a few minutes ago, before Tom walked into your office.

Tom is from Human Resources and he is reporting that an employee's bag was stolen from his gym locker. A company thumb drive was in the bag. Tom is coming to see you because the employee may have stored protected personal information on the thumb drive. You were recently named as the initial contact for potential data breaches in the company's incident response plan. To watch a video acting out this scenario, go to www.xtranormal.com/watch/11907723 (last visited August 11, 2011).

I have written [before](#) in *Business Law Today* on developing an incident response plan and what should be included in the plan. The basic concepts have not changed over the last few years. However, a few central questions still remain somewhat unclear. How do you know if there has been a data breach that requires notice? Who should be notified?

This article will discuss the little guidance available and suggest what should be the proper standard for when to provide consumer breach notifications. It will then discuss the initial investigation and

provide some guidance on conducting an investigation appropriate to the circumstances and geared toward addressing the legal questions. With this information in hand, a company is better positioned to decide whether a breach notice is legally required and who should be notified after a breach.

The Trend Toward Over Notification

The focus on data breach notification really began with the incident involving ChoicePoint in 2005. At that time, only California had a breach notification law. ChoicePoint decided initially to notify only California consumers. The backlash was swift and immediate. ChoicePoint quickly modified its decision and notified all affected consumers regardless of their state of residency. The lesson for the industry—err on the side of over notification.

Even in the wake of the ChoicePoint incident and the passage of numerous other notification laws by several other states, a debate emerged and continues to this day. Will over notification have an adverse effect on the purpose of the notice laws, namely causing consumers to disregard the notices? You may be able to answer this question based on your own experience from having received breach notices. Ask your neighbors, friends, and family. Most see the breach notice as another piece of junk mail and do little in response. Over

notification likely has not helped consumer's better protect themselves.

Guidance Provided by Notice Statutes

Learning from these lessons, it is time to take a closer look at when a security breach results in the need for consumer notifications. The initial investigation and the legal analysis become critical to reaching the correct decision. The place to begin is with the legal standard for providing notice. Admittedly, the states and regulators have not provided a clear picture on this point. As Sony can attest, making the wrong decision even today can have negative consequences.

The need to comply with the law of multiple states presents an interesting challenge. While most states followed the lead of California, many states added slight modifications that make the analysis (and thus planning for compliance) more complex. The same is true in this context. However, there are some common questions in deciding whether notice is required.

The obvious first question is whether the information at issue (i.e., personally identifiable information (PII)) is covered by the governing statute. Stated generally, breach notification laws concern data that includes some combination of personal identifying information (such as name and address) with confidential personal or financial information. The confiden-

tial information includes Social Security numbers, driver's license or state identification numbers, an account number in combination with a password or security code, medical information, and the like. In the end, only if the incident involves data covered by the notice statute is further analysis even required.

Once it is determined that protected information is at risk, then the next step is to determine if the information was accessed or copied. The most basic place to begin is whether the information was encrypted. Forty-six states do not require notice if the PII is encrypted. For example, under Nevada law (Nevada Revised Statute § 603A.215(5)(b)), encryption means "the protection of data in electronic or optical form, in storage or in transit, using: (1) An encryption technology that has been adopted by an established standards setting body . . . which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and (2) Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body. . . ." Notwithstanding any encryption protection of data, many of these states still require notice if the hacker had access to the encryption keys, i.e., the hacker could view the data regardless of the encryption.

If the encryption exception does not apply, then is notice automatically required? Is this the end of the investigation? No. Many states require some level of potential harm. For example, Arizona (Ariz. Rev. Stat. § 44-7501) requires that the breach "causes or is reasonably likely to cause substantial economic loss to an individual." Other states take a slightly different perspective. For example, Florida (Fla. Stat. § 817.5681) does not require notice if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the entity determines that there is no reasonable likelihood of financial harm to the consumer. Other states are silent on this point, such as Illinois, Georgia, and California.

A Framework for the Analysis

So what should be analyzed to decide if the harm element is met? The company should look at whether the information was accessed. If the company lacks records to determine definitively whether information was accessed, then a decision should be made as to the likelihood the information was accessed based on what data is available. Likewise, the company should determine whether the incident created a threat to the consumer. Was consumer PII the target of the unauthorized access?

An example helps illustrate the dynamics of this analysis. Suppose a criminal intends to steal money from the company. As part of the scheme, the criminal gains access to the company's computer system. The security breach could have given her access to PII. If there is evidence that (1) PII was not accessed or (2) consumer data was not the target of the scheme, then notice may not be required.

So why should notice not always be required? Think of the computer system like your home with many rooms, closets, chests, drawers, boxes, and any number of other places to store things. A burglar comes into your home. The burglar may have the run of your house or may be limited to certain rooms. When you come home, you want to see what was taken. You confirm that your locked rooms and chests were not compromised. You look at the areas where the criminal had access. You look to see what was missing and you call the police and your insurer. On the loss report, you claim only the items that are missing. The same should be true with a data breach. Notice should be required for only the information that you reasonably believe was at risk.

So how do you determine the risk to the consumer? You need to conduct a thorough and appropriate investigation. The obvious place to begin is interviewing the people involved. In our video scenario, you would interview the employee whose thumb drive went missing to learn such things as what data can he or she access, what did he or she store on the thumb drive, and what equipment was used to store information on the drive. You also

would interview the technical person supporting this employee to determine all of the locations in the company where copies of the data on the thumb drive are kept or where a footprint of what might be on the thumb drive might be located.

It is essential at the outset to identify and preserve all relevant records. Key sources that require immediate attention are log records and audit trails. If a third party handles any of the information or logs at issue, then a phone call and letter should be sent to secure these records. It is important to do this immediately as most systems allow such data to be written over within short periods of time (sometimes within 24 hours). These sources must be secured to avoid any spoliation issues, including any sources later identified by the entity conducting the forensic analysis.

You might ask loss prevention to speak with security at the gym where the bag was stolen. Likewise, if your employee has not done so already, then the employee should file a police report. Loss prevention should stay in contact with the police. These sources may be important to identifying the criminal and determining the target of the crime (although it is often too late to learn from the criminal what data was compromised).

Conducting a Forensic Study

Once you have a general understanding of the event, the next important step is to conduct a forensic analysis. I have written previously in this magazine on what issues should be considered in selecting the right party to conduct the study and some of the issues to consider. In sum, common issues include: (1) what application or process will be tested; (2) what type of data may be exposed, and what is the source of that data (questions important in identifying applicable laws); (3) who will conduct the testing, and have they been properly screened and educated as to the limits imposed by law or contract; (4) what techniques will be used, and do these techniques raise contractual or other compliance issues; and (5) who will receive copies of any reports, and what controls are in place to prevent dissemination to improper persons or for forbidden purposes.

The forensic analysis should be done under at the request of counsel so that the attorney-client privilege may be available to protect the results of the investigation from disclosure. With the above being said, the analysis should be done under the assumption that third parties will have access to the work papers and the final report. For example, Iowa and many other states require that a decision to not notify must be documented in writing and maintained for five years. Of course, if the decision is made to provide notice, then the company likely will want to claim privilege over this work.

The forensic analysis must be completed quickly. If notice is required, then the company must meet the timing obligations for such notice. For example, under Ohio law (Ohio Rev. Code § 1349.19(B) (2)), notification must be made “in the most expedient time possible but not later than 45 days following its discovery or notification of the breach in the security of the system. . . .” As a result, the focus of the study must be clear and controls must be put into place to prevent the investigation from losing sight of the main goals of the study. Indeed, the goals of the forensic analysis should be clear and direct: (1) determine if PII was accessed; (2) determine the target and mode of the attack; and (3) determine whose information may have been accessed. Regular meetings with the forensic team are essential. In my experience with system breaches, the answers to these questions often are complex, as data is stored in different places throughout a company’s systems. In analyzing a laptop matter, the difficulty is in recreating what was on the lost laptop.

Conclusion

The question of whether notice is required after a security breach should be given careful consideration. At the conclusion of the investigation, the team must consider all factors in deciding whether notice is required. Often there are close calls to be made. The company will need to balance not only whether notice is legally required, but also the public relation consequences of not providing notice. Likewise, the company may want to

consult the offices of the attorneys general that may have an interest in the ultimate decision (e.g., the state of the company; where large numbers of potentially effected consumers are located; and the states that provide national leadership on these issues).

While the standard is not clear or uniform, a reasonableness standard seems to have emerged. Over notification likely has defeated the purpose of breach notices. Lining up the law with the proper investigation of the facts will allow you to make the correct decision.

Ultimately, you want to give the consumers notice so that they can protect themselves, or if they have already been victimized, they will have some knowledge as to how it happened. Consumers can then take advantage of the assistance offered in the notice to protect them and remedy any potential harm. In the end, you should follow the Golden Rule—would you want to be notified if it was your information in the system?

Ronald I. Raether, Jr. is a partner at Faruki Ireland & Cox P.L.L. in Dayton, Ohio.

Additional Resources

For other materials on this topic, please refer to the following.

Business Law Today

Security Before and After a Data Breach

By Ronald I. Raether Jr.
Volume 16, Number 2
November/December 2006

Data Security and Ethical Hacking

Points to Consider for Eliminating Avoidable Exposure

By Ronald I. Raether Jr.
Volume 18, Number 1
September/October 2008

So Many Privacy Rules!

The Developing Standard of Care for Data Security and Identity Theft Protection

By Jonathan T. Rubens
Volume 18, Number 6 July/August 2009

From Private to Public Ordering

An Expanding Federal Role for Regulating Privacy and Data Security?

By Edward A. Morse
July 2011

2011 ABA Annual Meeting

Enforcement of Data Breach Notification Laws and Other Laws Safeguarding Personal Information:

Legal Perspectives from Both Sides of the Counsel Table

2011 Spring Meeting of the ABA Business Law Section

Privacy Police to Security Sheriffs:

The Emerging Federal Role in Regulating Privacy and Data Security Protection

Programs Prior to 2011

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Small Business and the Corporate Opportunity Doctrine

By [Mitchell L. Marinello](#) and [Christopher G. Dean](#)

The corporate opportunity doctrine prohibits a corporate fiduciary from exploiting an opportunity related to the corporation's business unless he or she first offers that opportunity to the corporation. There is no question whether the doctrine applies to small businesses. Indeed, countless cases confirm that it does. The more interesting question is how it applies, given the unique characteristics of many small businesses. In the small-business setting, challenges may arise as to whom, if anyone, the opportunity must be disclosed; whether the holder of a distributional interest in the business can challenge the business' decision to turn down an opportunity; what happens when basic corporate formalities are not followed; and whether the persons taking the opportunity have violated any duty to the business' creditors. This article explores those issues.

Rule of Disclosure

The officers, directors, and shareholders of a small business owe a fiduciary duty to their company that includes the obligation to refrain from usurping so-called corporate opportunities that rightfully belong to the company. A corporate opportunity exists when a proposed activity is reasonably related to the company's present or prospective business and is one in which the company has the capacity to engage.

The corporate opportunity doctrine is, in essence, a rule of disclosure: When a company's fiduciary wants to take advantage

of an opportunity that is in the company's line of business, "the fiduciary must first disclose and tender the opportunity" to the company. As the Supreme Court of Illinois explained in *Kerrigan v. Unity Savings Association*, 58 Ill. 2d 20 (1974), "[I]f the doctrine of business opportunity is to possess any vitality, the corporation or association must be given the opportunity to decide, upon full disclosure of the pertinent facts, whether it wishes to enter into a business that is reasonably incident to its present or prospective operations."

Despite the heavy emphasis the doctrine places on disclosure, the law of some states does not require the formal presentation of a potential opportunity when the company does not have any interest in pursuing the opportunity or the financial ability to engage in it. In *Broz v. Cellular Information Systems, Inc.*, 673 A.2d 148 (Del. 1996), for example, the Supreme Court of Delaware held that presentation is a form of safe harbor, "which removes the specter of a post hoc judicial determination that the director or officer has improperly usurped a corporate opportunity." The courts of other states, including George, Rhode Island, and Connecticut have adopted similar approaches.

But this "safe harbor" is not universal. Illinois courts, for instance, view the failure to disclose a corporate opportunity as undermining the "prophylactic purpose" of the rule. In such circumstances, the failure to disclose "forecloses" the

interested fiduciary from exploiting the opportunity, even in cases where he or she reasonably believes the company is incapable of claiming the opportunity. Thus, in *Kerrigan*, the court held that defendant-directors' belief that their savings and loan association was precluded by law from capitalizing on an opportunity in the insurance business could not "operate as a substitute for [their] duty to present the question" to the corporation for independent evaluation.

Application to Small Businesses

Disclosure of a corporate opportunity is, at least in theory, a simple process: The interested fiduciary tenders the opportunity to the company, fully discloses all pertinent information, and disinterested fiduciaries then evaluate whether the company should engage in the opportunity. The problem, however, is that this process does not always neatly apply in the context of a small business, where (1) each fiduciary may want to pursue the opportunity for himself; (2) distributional interests may be held by someone other than an owner; (3) corporate formalities are not always observed; and (4) the company may be insolvent or nearly insolvent.

Absence of Disinterested Fiduciaries

An interesting practical question can arise in small businesses when every owner knows about or is personally interested in the corporate opportunity. What happens

when there are no disinterested officers, directors, or owners to evaluate an opportunity on behalf of the business? Must the opportunity be presented to a disinterested third party for independent evaluation?

In re Tufts Electronics, Inc., 746 F.2d 915 (1st Cir. 1984) (Massachusetts law), was one of the first cases from any jurisdiction to consider this issue in detail. There, the former president, director, and sole shareholder (Martin) of a bankrupt corporation appealed from the judgment of the district court that had affirmed the imposition of a constructive trust on property he personally owned. Martin had acquired the property in part with corporate funds, and then leased the property back to his corporation. The bankruptcy and district courts had found that, under the corporate opportunity doctrine, Martin had breached his duty to the corporation by using corporate funds to help purchase the property for himself rather than for the corporation.

The First Circuit Court of Appeals disagreed. Emphasizing that Martin was the sole shareholder, director, and president of the company, the appellate court held that the corporate opportunity doctrine was inapplicable because Martin's actions "necessarily involve[d] the knowledge and assent of the corporation." The court further recognized that even though Martin and the corporation were separate persons, "absent some element of defrauding, Martin was not obliged, in every action he took, to prefer the corporation's interests to his own. No one could operate a corporation solely on such a basis."

A number of courts in other jurisdictions have applied similar reasoning to reach the same conclusions. For example, in *L.R. Schmaus Co. v. Commissioner of Internal Revenue*, 406 F.2d 1044 (7th Cir. 1969) (Wisconsin law), the court found that "if an officer of the company owns all the stock, he may use the corporate assets as he sees fit and there can be no misappropriation of corporate assets by him." Likewise, in *Mediators, Inc. v. Manney*, Adv. 93 Civ. 2304 (CSH), 1996 WL 297086, at *10 (S.D.N.Y. June 4, 1996) (New York law), the court dismissed a corporate opportunity claim because the

corporation had "necessarily consented" to diversion of its assets through the acts of its sole owners and officers, who were accused of usurping opportunity. To the same effect is *In Committee of Unsecured Creditors of Specialty Plastic v. Doemling*, 127 B.R. 945, 952 (Bankr. W.D. Pa. 1991), where the court reversed a usurpation finding because the corporate opportunity doctrine was "difficult to apply" to a small business where "there were no other shareholders to whom [the sole fiduciary] owed a duty of disclosure and loyalty." And in *Pittman v. American Metal Forming Corp.*, 649 A.2d 356 (Md. 1994), the court, upon surveying the law in other jurisdictions, held that the sole shareholder could not be liable for usurpation of a corporate opportunity in the absence of any harm to creditors.

The logic of these cases is compelling. After all, as the Seventh Circuit recognized in *In re Doctors Hospital of Hyde Park*, 474 F.3d 421 (7th Cir. 2007), a sole shareholder can "hardly . . . defraud[] himself or breach[] a fiduciary duty to himself." Other courts have reached the same conclusion, as in *In re Hearthside Baking Co., Inc.*, 402 B.R. 233 (Bankr. N.D. Ill. 2009) (a "sole shareholder does not owe a fiduciary duty against its own corporation and cannot breach a fiduciary duty to itself"); and *In re Gordon Car & Truck Rental, Inc.*, 65 B.R. 371, 376 (Bankr. N.D.N.Y. 1986) (corporate opportunity doctrine inapplicable where sole stockholders and officers "cannot be accused of withholding information from themselves").

A minority of courts have reached the same result through a different-but-related doctrine—ratification. For example, in *In re Safety International*, 775 F.2d 660 (5th Cir. 1984), the Fifth Circuit held that "even when [a] transaction is detrimental to the corporation, no cause of action will lie if all of the [interested] shareholders have ratified the transaction." According to the court, "[e]ven if [the directors/shareholders] breached their duty to [the corporation] by taking the purchase option in their own names, no party to this action can complain of the breach. There are no non-consenting shareholders."

In short, where the usurpation of a corporate opportunity from a small business necessarily involves the "knowledge and assent" of the corporation (*Tufts*) or ratification by the shareholders (*Safety International*), there can be no claim under the corporate opportunity doctrine. With the exception of insolvency, explained below, this rule is true even where the consenting or ratifying fiduciaries are personally interested in the opportunity.

Transfer of Distributional Interests

Many small businesses are structured as limited liability companies. A distributional interest in a limited liability company ordinarily is a transferable asset, and it is not uncommon for a member of an LLC to transfer his or her distributional interest to a person who has no ownership interest in the business, such as a creditor. That raises the question of how, if at all, such a transfer affects a fiduciary's disclosure obligations under the corporate opportunity doctrine.

The transfer of a distributional interest does not confer an ownership interest or a fiduciary relationship with the company's other members. The consequences of this are twofold. First, the transferee of a distributional interest is not entitled to exercise the rights of a member, which include challenging—either directly on its own behalf or derivatively on behalf of the company—the supposed usurpation of a corporate opportunity. Second, as a corollary, corporate fiduciaries are not obligated to disclose the opportunity to some independent third party for evaluation merely because a non-owner holds a distributional interest in the company.

In fact, the authors of this article recently defended the sole members of a limited liability company, a husband and wife, against a claim that the husband had usurped an opportunity of the LLC in precisely this situation. The usurpation claim was brought by a judgment creditor of the wife who had used part of its judgment to acquire her distributional interest in the company. The creditor argued that the husband could not take a corporate opportunity without first formally tendering the opportunity to the company and having

it evaluated by some independent person. According to the creditor, if the husband had not taken the corporate opportunity for himself, the company would have profited from the opportunity and would have had assets to distribute, which would have benefitted the creditor. The trial court rejected the creditor's argument. It found that the husband had no fiduciary duty to a creditor holding his wife's distributional interest in the LLC and, further, that the husband and wife, both of whom knew of the corporate opportunity, had no obligation to formally present the opportunity to the corporation or to submit it to an independent third party for evaluation. Accordingly, the court dismissed the claim.

Failure to Adhere to Corporate Formalities

The failure to adhere to basic corporate formalities, such as documenting meetings of the board of directors or recording shareholder votes, unfortunately is commonplace among many small businesses. This oversight is often a product of the cost of compliance, the casual approach to operations taken by many small business owners, or simple ignorance of proper procedure. Whatever its cause, a lack of documentation can lead to significant problems where corporate opportunities are concerned.

For example, take a situation where every shareholder knows of a corporate opportunity, and agrees that the business should not pursue it. Some of the shareholders decide to take the opportunity for themselves, but they fail to document any sort of formal presentation of the opportunity to the business or official vote of the officers or directors. Sometime thereafter, perhaps because the business opportunity turns out to be better than expected or because the shareholders have a falling out over an unrelated issue, the shareholders who did not take the corporate opportunity bring a lawsuit against those who did claiming that the opportunity was not fully or properly disclosed to the corporation.

What might have been quickly resolved with proper documentation had corporate formalities been observed now presents a thorny factual issue. Was the opportunity

actually tendered to the corporation? Were the pertinent facts fully disclosed? Did the board or shareholders in fact agree that the business should not pursue it? The fact that the answers to these questions cannot be found in board meeting minutes or shareholder ballots could mean the difference between a speedy resolution of the claims on a motion to dismiss and costly, time-consuming discovery. In short, the failure to adhere to corporate formalities that so often plagues small businesses can make a mountain out of a mole hill in the context of a usurpation claim.

Insolvency

An additional consideration is whether the small business was solvent at the time of the challenged transaction. This is important because, when a company is insolvent, the duties of its fiduciaries—including the duty to disclose corporate opportunities—extend to its creditors. As the Supreme Court of Delaware recently explained in *North American Catholic Educational Programming Foundation, Inc. v. Gheewalla*, 930 A.2d 92 (Del. 2007):

It is well settled that directors owe fiduciary duties to the corporation. When a corporation is *solvent*, those duties may be enforced by its shareholders, who have standing to bring *derivative* actions on behalf of the corporation because they are the ultimate beneficiaries of the corporation's growth and increased value. When a corporation is *insolvent*, however, its creditors take the place of the shareholders as the residual beneficiaries of any increase in value.

And once an insolvent company files for bankruptcy, its creditors have standing to complain about the usurpation of corporate opportunities, and they often do. A small business is no different than any larger company in this respect.

In re McCook Metals, LLC, 319 B.R. 570 (Bankr. N.D. Ill. 2005), illustrates the point. There, the bankruptcy trustee of a closely-held aluminum processor (McCook) brought suit against McCook's principal (Lynch) for, among other things, transferring an opportunity to acquire a smelter away from McCook. As part of his defense, Lynch argued that he had

breached no duty to McCook because he had disclosed the opportunity to purchase the smelter to McCook's other members, who agreed that a separate entity should make the acquisition. The bankruptcy court rejected this argument because the duty involved was to McCook's creditors, not its other members. According to the court, "That the other member owners agreed to transfer the [smelter] opportunity away from McCook makes them jointly and severally liable, with Lynch, for a breach of duty to the creditors; it does not excuse Lynch."

Similarly, in *Brown v. Presbyterian Ministers Fund*, 484 F.2d 998 (3d Cir. 1973), the president and majority shareholder (Hoffman) of a family-owned business arranged to personally buy a mortgage at a discount when the opportunity to do so rightfully belonged to his corporation. The corporation filed for bankruptcy hours after the purchase was complete. The district court found that Hoffman had not breached a duty because the acquisition was agreed to with the "knowledge and approval of all of [the corporation's] officers, directors and shareholders," i.e., Hoffman and his sons. The Third Circuit rejected this logic, finding that it could not "countenance such a narrow view of the scope of Hoffman's fiduciary duty. As an officer, director and principal stockholder of an insolvent corporation . . . Hoffman was duty bound to act with absolute fidelity to both creditors and stockholders." The court explained that because Hoffman had arranged the transaction with knowledge of his corporation's insolvency, approval by the fiduciaries did not free him to appropriate corporate opportunities to the detriment of the corporation's creditors. Corporate assent did not, therefore, relieve Hoffman of his fiduciary duties, and the "opportunity should have been disclosed to the receiver as representative of the creditors."

Conclusion

The corporate opportunity doctrine can pose significant challenges to the owners of small businesses. These problems can be exacerbated by the failure to observe corporate formalities and, in particular,

whenever the corporation is insolvent and the rights of creditors are at stake. Still, when insolvency is not an issue, there is case law support for the notion that small business owners have the right to treat their business as their own, including by taking corporate opportunities for themselves personally.

Mitchell L. Marinello is a partner and Christopher G. Dean is an associate at Novack and Macey LLP in Chicago.

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Insider Trading by Friends and Family: When the SEC Alleges Tipping

By Dixie L. Johnson and Robert Greffenius

Imagine the horror: a corporate executive confides in a family member, sharing information about her career (and, therefore, about her company), and the family member trades in the company's securities. Or a young professional shares a house with a friend, who pieces together what the professional is working on and trades. Government insider trading investigations ensue, the traders are charged, and lives are changed, all because of an inadvertent tip. And, because these cases are built on circumstantial evidence and credibility assessments, there is always the risk that the government could take the view that the tips were not inadvertent, and could charge the corporate executive or young professional with tipping, furthering the nightmare.

Ideally, of course, everyone could trust family members and friends to make good decisions and not act in a way that could put themselves and loved ones in danger. And ideally, the government would charge only people who actually violated the law. Unfortunately, the ideal is not always the reality; unless sensitive information is protected carefully, corporate insiders and service providers retained by companies to whom sensitive corporate information is entrusted risk government investigations that can wreak havoc on personal and professional lives. The current economy compounds this situation, increasing the temptation of easy money through insider trading. For those hit

hardest economically, and with access to nonpublic information through a friend or family member, the lure may become especially hard to resist. Understanding the risk, and taking steps to protect against it, could save heartache—and worse—down the road.

How Liability is Determined

It is important to understand the contexts in which those who possess material nonpublic information risk liability for disclosing it. Any tipping case could be prosecuted by the criminal authorities if the level of proof is sufficient to establish guilt beyond reasonable doubt; the Securities and Exchange Commission faces a lower burden of proving its allegations by a preponderance of the evidence. Due to the heavy burden of proof required of criminal prosecutors and other high priority crimes they also must address, most tipping cases are brought by the SEC. Although some defendants litigate, many cannot afford the monetary and emotional cost of doing so, and most tipping cases brought by the SEC settle with the defendant neither admitting nor denying the SEC's allegations.

The law, section 20A of the Securities Exchange Act of 1934, provides that a tipper is jointly and severally liable with his or her tippees (both direct and indirect) for the ill-gotten gains (or the losses avoided) those tippees obtained as a result of the tip, plus interest. The tipper also may face a

monetary penalty of up to three times the amount of those ill-gotten gains or losses avoided, although most cases settle for a one-time penalty equal to the disgorgement amount. Taken to an extreme, the tipper need not know anything about the trades themselves or have any voice in the dollar amounts at issue—the tipper can be liable for dollar amounts in the thousands, millions, or even more for trading profits or losses avoided that he or she never received, shared, or even knew about.

The elements of a tipping charge are not statutory; they have evolved in case law interpretations of the Exchange Act section 10(b) and Rule 10b-5 thereunder. To allege tipping, the government must prove that the tipper had material, nonpublic information; that he or she had a duty (as a company employee, or as a lawyer, accountant, banker, or other service provider retained by the company) to maintain the information as confidential; that the tipper communicated the information to someone who traded or tipped others to trade; and that the tipper intended to benefit personally by giving the tip.

The crux of assessing potential tipping liability often centers on the "personal benefit" element. The SEC and various courts have construed the concept of a personal benefit very broadly. As a result, for such a significant allegation, the level of proof required in this "personal benefit" test is shockingly low. The United States

Supreme Court has stated that, when the person who possesses the information passes it to a tippee, the SEC may prove intent to benefit through (1) receipt of pecuniary benefit (e.g., profits from the trading), (2) receipt of a “reputational” benefit, or (3) provision of the information as a “gift” to the tippee.

Although some cases turn on whether profits were shared, such circumstances are not generally thought to be controversial as the sharing of trading profits can be a hallmark of an improper trading scheme. Thus, it is the second and third avenues that pose the biggest problems for those who possess inside information because those avenues are less susceptible to having precise definitions or clear criteria. Charging decisions can turn on subjective assessments of suspicious government attorneys. For example, in *SEC v. Stevens*, No. 1:91-CV-01869-CSH (S.D.N.Y. Mar. 19, 1991), the SEC secured a settlement against a tipper under a reputational benefit theory when a CEO allegedly provided material nonpublic information to an investment analyst with the “hope” that the analyst would issue favorable reports about the CEO’s company in the future. Under a “gift” theory, the Supreme Court in *Dirks v. SEC*, 463 U.S. 646 (1983), reasoned that information imparted to a friend or family member “resembles” insider trading by the officer or director him or herself with a subsequent gift of the proceeds to the tippee. As the gift doctrine has expanded, it has incorporated acts such as those intended “to effect a reconciliation with [a] friend and to maintain a useful networking contact.” *SEC v. Sargent*, 229 F.3d 68, 77 (1st Cir. 2000). These examples demonstrate that the personal benefit test is a malleable concept that, in the event of seemingly timely trades, risks opening a relationship to government scrutiny.

Unfortunately, determining the exact contours of the intent to benefit prong under an enhancement of reputation or bestowal of a gift theory is very difficult. Courts rarely find a lack of a gift where one is alleged, although this has occurred when a court concluded that an alleged tipper did not intend for the tippee to hear the information, and when there was no evidence of any personal relationship between the

tipper and the tippee.

In some cases, the SEC may not charge the corporate insider or service provider for having tipped, and instead may pursue the trader on a misappropriation theory only, meaning the trader obtained the material nonpublic information in a manner that did not give the insider or service provider any reason to believe that person would trade. This could occur if the insider or service provider did not intentionally or recklessly provide the information, or it could occur if the insider or service provider intentionally communicated the information for a different purpose and did not intend for the recipient to trade. Under a misappropriation theory,

a person commits fraud ‘in connection with’ a securities transaction, and thereby violates § 10(b) and Rule 10b-5, when he misappropriates confidential information for securities trading purposes, in breach of a duty owed to the source of the information . . . In lieu of premising liability on a fiduciary relationship between company insider and purchaser or seller of the company’s stock, the misappropriation theory premises liability on a fiduciary-turned-trader’s deception of those who entrusted him with access to confidential information.

SEC v. Talbot, 530 F.3d 1085, 1091 (9th Cir. 2008) (quoting *United States v. O’Hagan*, 521 U.S. 642, 652 (1997)). Close family relationships carry with them a duty to the source of the information, and may therefore give rise to insider trading liability. While an SEC action against a trader under a misappropriation theory may spare the corporate insider or service provider from legal actions against him or her personally, it nevertheless can have significant collateral consequences in his or her life. The insider’s or service provider’s relationship with the trader will be, in many cases, irreparably damaged, and the insider’s or service provider’s relationship with his or her employer, in many cases, comes to an end.

Several recent cases have highlighted the dangers associated with friends and family trading on information directly or indirectly gleaned from a corporate

insider. These cases serve as examples of the risks associated with holding material nonpublic information as well as important lessons on how best to prevent trades based on such information.

Apparently Inadvertent Disclosure

Although the category of friends and family insider trading cases has existed for as long as insider trading cases themselves, new lawsuits continually highlight the dangers that an insider’s closest relationships can pose. The facts alleged in two recent cases, *SEC v. Goetz*, No. 3:11-CV-01220-IEG-NLS (S.D. Cal. Jun. 3, 2011), and *SEC v. Haim*, No. 3:11-CV-02958-MLC-LHG (S.D.N.Y. May 24, 2011), which settled without the defendants admitting or denying the allegations, are recent examples. In *Haim*, the defendant, a relative of an investment banker, allegedly eavesdropped on telephone calls and read documents while visiting the investment banker’s New Jersey home. Mr. Haim’s alleged trades in the securities of five companies stretched from April 2006 until March 2007, and the SEC settlement required a disgorgement of \$30,126, pre-judgment interest of \$7,188, and a penalty of \$30,126.

The *Goetz* relative was a young attorney’s father. According to the complaint, in December 2008, the young attorney worked in the Los Angeles office of a large international law firm, and she spent two weeks at her parents’ home for the holidays. While visiting, she continued to work on a merger transaction between her firm’s client, Advanced Medical Optics, and Abbott Laboratories, set to close in January 2009. She worked on aspects of the due diligence for the transaction in various locations around her parents’ home, sometimes borrowing the office desk of her father, Dean A. Goetz, who was also an attorney. Some of the documents on which she worked included disclosure schedules which, unlike most of the merger documents, identified one of the parties by its actual name. Unbeknownst to his daughter, Mr. Goetz accumulated sufficient information from her documents, and, likely, from her announcement upon cutting her visit

short that “[h]opefully we’ll close soon,” to confirm the identity of one of the merging companies and the timing of the transaction.

Mr. Goetz allegedly misappropriated this information and purchased shares in the merging company in the early afternoon of the day the merger was scheduled to be announced using a trading account he had not used in nearly a year. Once Mr. Goetz sold his shares after the merger announcement, his profits totaled \$11,418. Although this was a relatively small sum compared to many other cases the SEC has brought, on June 3, 2011, the SEC charged Mr. Goetz and argued that he had misappropriated his daughter’s material, nonpublic information by breaching his family duty of loyalty and confidentiality. Mr. Goetz’s settlement included disgorgement of his profits, prejudgment interest, and a penalty equal to his profits, for a total of \$23,761.65. The complaint named only Mr. Goetz, but we can be certain that the daughter was required to participate in the SEC’s investigation in relation to the disclosure.

Allegedly Intentional, Confidential Disclosure

A similar story played out in Connecticut, although in this case the insider allegedly intended to disclose facts to the family member, who in turn misappropriated the information by trading for himself and by tipping others who then also traded. According to the facts alleged in this February 2010 case, *SEC v. Macdonald*, No. 3:10-CV-00151-CFD (D. Conn. Feb. 1, 2010), which Bruce Macdonald, Robert Maresca, and Bruce Bohlander settled without either admitting or denying the allegations, Mr. Macdonald’s wife was employed as the corporate secretary and vice president of human resources of Memry Corporation, a medical device company. While Mrs. Macdonald was serving in this capacity, Memry began seeking out suitors to buy the company, and negotiations evolved throughout 2007 and into the first half of 2008. Since Mrs. Macdonald was part of senior management, she was included in several important steps of the due diligence process, and she frequently

updated her husband on the progress of the sale. In September 2006, the company instructed its employees that they were under a “blackout” from trading company shares for an indefinite period, and Memry recirculated the blackout notice the following year on September 30, 2007, and November 16, 2007. Mrs. Macdonald relayed such blackout restrictions to her husband because he was in charge of the family’s trading accounts.

The SEC alleged that, without telling his wife, Mr. Macdonald used the account of a small business that he owned and the account of a childhood friend, Mr. Bohlander, to purchase shares on numerous dates over a several-month period beginning on July 13, 2007, the day after the board meeting concerning the process for hiring an investment bank, until April 4, 2008, over a month after on-site due diligence began. Memry did not announce the merger plan until June 24, 2008. Even though Mr. Macdonald ceased trading more than two months before the merger was announced, the SEC’s allegations centered on several of Mr. Macdonald’s trades, which coincided in date with important stages of the merger process. Mr. Macdonald also allegedly alerted three friends, co-defendant Mr. Maresca and two others who are not named or charged in the complaint. To Mr. Maresca, Mr. Macdonald said he should “[b]uy Memry stock. You don’t want to know why.”

As in *Goetz*, the SEC pursued a misappropriation theory, charging Mr. Macdonald and Mr. Maresca in February 2010 with insider trading, but not charging Mrs. Macdonald with tipping. Again, the profits were relatively slim: Mr. Macdonald’s small business account earned a profit of \$890, Mr. Bohlander’s account earned \$25,508, Mr. Maresca earned a total of \$12,335, and the two other tippees received total profits of \$7,307.50.

Although five people allegedly profited, only Messrs. Macdonald and Maresca were charged with violating the law. The SEC named Mr. Bohlander as a relief defendant and required him to pay disgorgement of \$25,508 and prejudgment interest of \$1,748, but did not charge him with a violation, presumably since Mr. Macdonald

had trading authority over his account. The two other traders were not named, and Mr. Macdonald was required to disgorge their profits himself, along with those in his business account. Mr. Macdonald’s penalty covered his own trades, including the trades on Mr. Bohlander’s account, but he was not penalized for the profits of the unnamed traders. Mr. Maresca disgorged his own profits, interest and a one-time penalty.

In another, more recent example of one spouse trading on inside information learned from the other, the SEC recently charged William Marovitz, the husband of Christie Hefner, the former CEO of Playboy Enterprises, Inc., with insider trading in the case of *SEC v. Marovitz*, No. 1:11-CV-05259-JWD (N.D. Ill. Aug. 3, 2011). According to the SEC, Mr. Marovitz made multiple trades between 2004 and 2009 based on material nonpublic information that he learned from his wife, despite her own expressed concern about his trading in Playboy stock and despite Playboy’s general counsel’s warnings not to trade in Playboy stock without first consulting him. For example, in 2009, Mr. Marovitz allegedly bought stock after having learned of Iconix Brand Group, Inc.’s interest in buying Playboy before it was publicly reported, and sold stock prior to the public announcement that Iconix was breaking off merger talks. Mr. Marovitz also allegedly traded in advance of two negative earnings releases and a 2004 public stock offering. Mr. Marovitz settled these allegations without admitting or denying the charges, agreeing to disgorge profits and losses avoided in the amount of \$100,952. Mr. Marovitz’s total disgorgement, prejudgment interest, and civil penalties amounted to \$168,352. Thus, it appears that the terms of Mr. Marovitz’s settlement required a civil penalty of approximately one half of his profits gained and losses avoided. The settlement must still be approved by the court.

Although neither spouse was charged personally, Mrs. Macdonald and Ms. Hefner must have been intimately involved in the investigations into their husbands’ conduct, and such investigations are an emotionally and financially draining experience, at a minimum.

Liability Despite No Trading by Tippee
This 2011 case involved Kim Ann Deskovick and Brian S. Haig, who settled the SEC's charges without admitting or denying its allegations. According to the complaint in *SEC v. Deskovick*, No. 2:11-CV-01522-JLL-CCC (D.N.J. Mar. 17, 2011), in early 2006, Ms. Deskovick was serving as the director of a regional bank in New Jersey. During this time, Ms. Deskovick hired an unnamed individual to perform services on her home and the two "developed a close personal relationship." In mid-2006, the regional bank for which Ms. Deskovick served as a director decided that, in light of its decreasing revenues, it should search for a buyer. Ms. Deskovick's position at the bank not only made her aware of the bank's intent to find a buyer, but gave her access to confidential information about the progression of the deal. In March 2011, the SEC charged Ms. Deskovick with tipping inside information. Allegedly, Ms. Deskovick informed the unnamed individual about the impending sale and kept him informed as the deal moved forward. This unnamed individual allegedly tipped the inside information to his accountant, Mr. Haig, informing Mr. Haig that his friend "Kim" alerted him to the sale.

The SEC's complaint stated that Ms. Deskovick telephoned the unnamed individual "in close proximity to several key events in the transaction," after which the unnamed individual called Mr. Haig who then purchased stock. For example, the SEC alleged that Ms. Deskovick called the unnamed individual while he and Mr. Haig were having dinner with their spouses and told him that an agreement had been completed and an announcement was imminent, information that the unnamed individual conveyed to Mr. Haig. The following day, the acquisition was announced publicly, and Mr. Haig made a profit of \$56,797 after selling his shares.

The SEC's charges against Ms. Deskovick rested on a "gift" theory, alleging that Ms. Deskovick had knowledge that the unnamed individual had been in financial difficulty, she had helped him monetarily between March and July 2006, and she gave his wife gifts. The complaint does not

allege that the unnamed individual ever traded on Ms. Deskovick's information, but the SEC apparently concluded that Ms. Deskovick's alleged intent to confer a gift provided the element necessary to pursue her for tipping. The SEC's allegations as far as Mr. Haig were concerned rested entirely on the timing of phone calls among Ms. Deskovick, the unnamed individual, and Mr. Haig, as well as the timing of Mr. Haig's trades. While Mr. Haig was ordered to pay disgorgement of \$68,277, equal to his profits plus the profits of the deceased individual whom Mr. Haig had tipped, prejudgment interest of \$18,007, and a civil penalty of \$34,138, Ms. Deskovick also consented, without admitting or denying the allegations, to paying a civil penalty of \$68,277 (an amount equal to Haig's and the deceased individual's profits). Ms. Deskovick was also barred from serving as an officer or director of a public company for five years.

Instead of pursuing a misappropriation theory, the SEC in *Deskovick* alleged that the defendant herself had breached her fiduciary duty by passing information to the individual who ultimately tipped Mr. Haig. However, the SEC did not allege anything beyond circumstantial evidence that Ms. Deskovick intended to confer financial benefit on her friend, who did not ultimately trade in the stock. And, unlike in *Goetz* or *Macdonald*, the insider herself suffered direct, legal consequences as a result of conversations she had with a friend, to say nothing of any personal, non-legal consequences she may have suffered.

Conclusion

So what can be learned from these cases? Most people's natural tendencies make them inclined to believe the best about people, especially those with whom they are closest and who they trust the most. Ironically, because the showing of a close, personal relationship is frequently sufficient to show the intent to convey a benefit, friends and family members pose the greatest potential risk to corporate insiders and service providers who confide confidential corporate information in them.

While it is of course wise to avoid discussion of material nonpublic company

business with friends and family, some of the cases discussed above show that silence may not always be enough. Family members and friends might be deterred by discussions of what could happen if they tread in these waters, but dishonest people can find a way to misappropriate material nonpublic information if they are determined. The current financial environment could increase the risk that people, even trusted family members and friends, may succumb to the temptation to try to analyze pieces of information shared with them and to take advantage of such information by trading upon it.

This is a good time to remind corporate executives to provide information only to those who need to know it, and to renew efforts to protect information that might be accessible to family or friends who could be tempted to trade. They may also want to consider password protecting home computers, personal computing tablets, telephones and/or individual files that store the information, and keeping hard copies of documents either at work or locked in filing cabinets at home. These cases also serve as a good reminder to corporate counsel that insider trading policies should be clear and frequently circulated, that confidential documents should be marked as such and distributed only to those who need to know the information, and that clear warnings are issued to people when they receive material nonpublic information from their employer. These cautionary tales show that even when a corporate insider believes that the risk of betrayal is small, it is still good practice to take extra precautions to reduce exposure.

Dixie L. Johnson is a partner and *Robert Greffenius* is an associate in the Washington, D.C., office of Fried, Frank, Harris, Shriver & Jacobson LLP.

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Keeping Current: Class Actions

Supreme Court Deals a Heavy Blow to Colossal Class Actions

By [M. Carter Crow](#) and [Brian S. Greig](#)

On June 20, 2011, the United States Supreme Court handed down the long-awaited decision in *Wal-Mart v. Dukes*, No. 10-277, 564 U.S. ___, 2011 US LEXIS 4567 (2011) (Scalia, J.), which reversed class certification in what is believed to be the largest class action certified in the United States. The decision is a victory for businesses defending against massive class actions, and employers in particular. After a series of employee-friendly decisions, the United States Supreme Court has rendered a decision in favor of large employers with widespread operations.

According to the class representatives, although the 1.5 million women in the class had different supervisors in different stores at different times, held different positions, and were subject to different decisions, they had one common complaint. Specifically, they contended that a company-wide "policy" of allowing local managers to use discretion in pay and promotion decisions resulted in across-the-board discriminatory decisions.

The Supreme Court's decision to reverse the class certification was unanimous, but the justices divided as to why. The majority and dissent vigorously disputed that the plaintiffs' proof of decentralized, subjective, decision-making—allegedly coupled with a centralized yet pervasive culture and policies—was sufficient to support the aggregation of millions of claims by women from 3,400 Wal-Mart facilities nationwide who were

seeking billions of dollars of back pay and injunctive relief based on alleged gender discrimination in promotion and pay.

Common Proof of Discrimination

The employees pursued both disparate impact and disparate treatment claims—disparate impact because the practice of granting discretion to local managers allegedly caused a disproportionately adverse effect on females, and disparate treatment because Wal-Mart allegedly knew about this adverse impact yet failed to correct it.

The Court held that the proposed class failed for lack of common questions under Rule 23(a). Specifically, the Court required proof of a specific employment practice that tied the class members' claims and common experiences together, which it found lacking in the case presented: "Merely showing that Wal-Mart's policy of discretion has produced an overall sex-based disparity does not suffice." For purposes of certifying this nationwide class, the "crux of this case [was] commonality." Federal Rule of Civil Procedure 23(a)(2) requires the trial court to find common questions of law or fact as a threshold matter in order to certify a class. According to the Court, the commonality question asks not whether all of the 1.5 million female employees had managers with discretion over their pay or promotions, nor whether they believed such discretion led to unlawful acts under

the same provision of Title VII. The Court found the key to class action treatment was not whether common questions could be posed, but rather whether a class proceeding could generate common answers that would resolve the litigation.

An example of a truly common question is when employees assert discriminatory bias on the part of the same supervisor, which makes sense when considering that disparate treatment authorities typically require an employee claiming discrimination to show someone outside of his or her protected class received preferential treatment in nearly identical circumstances. Employers have long defended such claims by demonstrating that the employee's proffered comparator was invalid or irrelevant because it involved a different supervisor or different circumstances. In *Dukes*, the Supreme Court reaffirms the principle that an employee's claim of intentional discrimination is a fact intensive inquiry into what actually happened for that particular employee—it is not an issue that can be decided by anecdotes from other employees in other unrelated circumstances.

The four-justice dissent charges the majority with "disqualify[ing] the class at the starting gate," by elevating the standard for common questions to an unrealistic and unprecedented level. According to the dissent, the majority's framing of the common question precluded the Court from giving sufficient deference to the trial

court's findings of fact. Justice Ginsburg surveyed the evidentiary landscape, concluding that the questions identified were in fact common under Rule 23(a)(2).

Dukes does not hold that class actions as a whole are inappropriate for intentional discrimination claims. Rather, to establish sufficient commonality for a discrimination class action, employees may show that an employer used a biased testing procedure, or they may provide "significant proof that an employer operated under a general policy of discrimination[.]"¹ The Court rejected the argument that allowing local managers discretion in pay and promotion decisions was a "common" policy of discrimination. Instead, it reasoned that granting managers discretion was:

on its face . . . just the opposite of a uniform employment practice that would provide the commonality needed for a class action; it is a policy against having uniform employment practices. It is also a very common and presumptively reasonable way of doing business—one that [the Court has] said 'should itself raise no inference of discriminatory conduct'

Justice Scalia provided examples of how different managers could use discretion differently: by using sex-neutral, performance-based criteria; by using test scores or education criteria; or by using discriminatory motives. "In such a company, demonstrating the invalidity of one manager's use of discretion will do nothing to demonstrate the invalidity of

another's. A party seeking to certify a nationwide class will be unable to show that all the employees' Title VII claims will in fact depend on the answers to common questions."

The Court found no single common question existed, and the employees had no convincing proof of a company-wide discriminatory pay and promotion policy. Rather, the "class" involved a multitude of different employees with different jobs at different levels for different periods of times in different stores in different states with different supervisors subject to different policies. Quoting from Judge Kozinski's dissent in the Ninth Circuit, the Court agreed that: "[s]ome thrived while others did poorly. They have little in common but their sex and this lawsuit."

Implications of *Dukes* Decision

While this decision is a major victory for employers, it also underscores the importance of having company policies forbidding discrimination. Indeed, the Court noted in the decision that Wal-Mart forbade discrimination and penalized employees who violated equal employment opportunity laws. The Court focused on the fact that the conduct alleged would have been contrary to company policy, countering the assumptions the plaintiffs asserted that managers would discriminate if left to their own choice and that there existed of an unwritten policy of discrimination contrary to the express policy. We also learn from *Dukes* that treating employees as individuals buttresses

an employer claim that its defenses to discrimination may vary from employee to employee, not a circumstance for class treatment.

In the high-stakes world of complex litigation, courts, commentators, and practitioners alike have been wrestling with a number of vexing issues. In particular, consumer and labor class actions in particular have been on the rise—between 2001 and early 2007, they have increased 156 percent and employment class actions have increased over 200 percent. The trend has been growing against certification of class actions due to considerations of individual rights of both the plaintiffs and defendants, but the need for some sort of aggregate resolution of litigation stemming from mass disasters, wide-reaching business practices, and pervasive schemes has outpaced the historical judicial restraints. The *Dukes* decision is expected to reverse this trend and significantly limit the number of classes appropriate for certification. Its impact should also reach beyond the federal courts, as many states have patterned their class action practices on Federal Rule 23 and look to federal authorities as guidance for interpretation of their local rules.

M. Carter Crow and Brian S. Greig are partners in both the Litigation and Labor and Employment Practice Groups of Fulbright & Jaworski L.L.P.

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Keeping Current: Securities

SEC Fines Three Brokerage Executives for Regulation S-P Violations

By [Marc J. Lederer](#)

For the very first time, the Securities and Exchange Commission (SEC) has assessed financial penalties against individuals charged solely with violating Regulation S-P. As part of an agreement to settle the SEC charges against them for failing to protect confidential information about their customers, a former president and sales manager of a now defunct brokerage dealer have been each ordered to pay penalties of \$20,000, and the former Chief Compliance Officer (CCO) of the firm paying \$15,000.

Background

GunnAllen Financial Inc. (GAF) was registered as a broker-dealer with the SEC from March 1986 to April 2010. As its business was winding down in 2010, GAF's Sales Manager, David C. Levine, planned to form with another GAF representative a new business partnership and intended to transfer GAF's customer accounts as an incentive for another broker-dealer to employ them. To that end, GAF's president, Frederick O. Kraus, authorized the transfer of 16,000 accounts containing nonpublic personal information (NPI) of its customers to any broker-dealer that Levine and his partner chose to associate with after they left GAF. On May 14, 2010, Levine sent those GAF customers a letter notifying them that their accounts would be transferred to another broker-dealer in which Levine was newly associated (the Receiving BD) unless those customers decided to opt-out within

15 days. Before verifying whether any customers had chosen to opt-out, Levine provided the NPI contained in the GAF accounts to the Receiving BD.

GAF's Violations of Regulation S-P

Rule 7(a) and Rule 10(a) of Regulation S-P essentially prohibit SEC registered broker-dealers from disclosing the NPI of their customers without first providing them with a clear and conspicuous notice of the broker-dealer's privacy practices and an explanation of the customer's opt-out rights, as well as provide the customers with a reasonable opportunity to opt-out of any disclosure. The SEC alleged that GAF violated Rule 7(a) and Rule 10(a) by failing to provide its customers with notice of their opt-out rights, and by not notifying them that their account information was transferred until after the disclosure of NPI to the Receiving BD had already occurred. Moreover, the SEC claimed that GAF did not provide a sufficient time for its customers to opt-out and that it was unreasonable to only provide for opt-out objections through a letter that the customers had to write to GAF.

In addition, Rule 30(a) of Regulation S-P (otherwise known as the "Safeguards Rule"), requires broker-dealers to maintain reasonably designed policies and procedures to protect the NPI of their customers from security threats and unauthorized access. The SEC alleged that GAF violated the Safeguards Rule by not putting in place policies and procedures

to address the transfer and protection of its customers' NPI, despite the reasonably foreseeable risk that its departing registered representatives would disclose customer NPI to successor brokerage firms during GAF's winding-down period.

Violations by the Individual Executives

As a result of Levine's actions in transferring GAF customer accounts and NPI to the Receiving BD and sending untimely and inadequate notices to those customers, the SEC alleged that Levine willfully aided and abetted and caused GAF's violations of Rules 7(a), 10(a), and 30(a) of Regulation S-P. Pursuant to the settlement with the SEC, he was ordered to pay a monetary penalty in the amount of \$20,000, was censured, and was required to cease and desist from committing or causing any violations or future violations of the provisions charged.

The SEC also alleged that Kraus willfully aided and abetted and caused GAF's violations of Rules 7(a), 10(a) and Rule 30(a) of Regulation S-P as a result in of his role in authorizing the transfer of the 16,000 customer accounts and their NPI to Levine and in approving the contents of the inadequate and untimely notifications to such customers. Kraus also settled with the SEC by agreeing to pay a monetary penalty in the amount of \$20,000, consenting to censure and ordered to cease and desist from committing or causing any violations or future violations of the provisions charged.

Finally, the SEC found that GAF's CCO, Marc A. Ellis, willfully aided and abetted and caused GAF's violations of Regulation S-P's Safeguards Rule. As GAF's CCO, Ellis was responsible for implementing, maintaining, and reviewing its policies and procedures in order to comply with the Safeguards Rule. The SEC believed Ellis should have been on notice that GAF's policies and procedures were inadequate to comply with the Safeguards Rule as a result of previous unrelated incidents in which laptop computers were stolen and an employee's password credentials were misappropriated. Indeed, the SEC found that GAF's safeguarding policies and procedures were too short (less than a page long), general, and too vague, and failed to address the transfer and protection of customer NPI. As with the other former GAF executives, Ellis settled with the SEC and was ordered to pay a monetary penalty in the amount of \$15,000, was censured, and was required to cease and desist from committing or causing any violations or future violations of the Safeguards Rule.

Practical Implications

This settlement should remind senior officers of financial institutions that the SEC is willing to hold them individually liable for their role in violations of Regulation S-P. Therefore, it is incumbent upon such individuals to consider the effect of their actions and of their company's decisions regarding the privacy rights of customers. Lastly, companies and their executives should also take away from this settlement that the SEC will consider whether an information security policy is sufficiently comprehensive when determining Regulation S-P liability.

Marc J. Lederer is a privacy law attorney at the New York office of Willkie Farr & Gallagher LLP

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Keeping Current: Patents

Will America Reinvent Itself? Patent Reform in 2011

By [Gregory N. Mandel](#)

Congress has considered significant patent reform legislation every year since 2005, and every year the proposed reforms have produced vociferous debate among the United States' largest industries. The debates over whether patent rights should be weakened, strengthened, or otherwise modified have spilled over from lobbying efforts into litigation and the media. To date, none of the patent reform bills have passed. Patent legislation introduced this year, the "America Invents Act" (S. 23, 112th Cong. (2011); H.R. 1249, 112th Cong. (2011)), incorporates a more modest set of reforms and has been met with broader backing. The America Invents Act passed the Senate in March 2011 and a similar counterpart bill passed the House in June. It appears likely that the chambers will reconcile their bills, and with the White House's strong support, this may finally be the year that patent reform is enacted. If enacted, the America Invents Act will represent the most sweeping statutory changes to patent law in over half a century.

Can Patents Produce a Drag on Innovation?

To understand the import and likely effects of the America Invents Act it is necessary to take a step back to understand how the legislation developed. The essential policy behind patent law is relatively straightforward. Absent patent protection, there would be too little incentive to invent and commercialize innovation because, once introduced, anyone could

copy an invention without having to compensate the inventor. Inventors, as a result, would be unable to recoup their research and development costs, and therefore would be less likely to invest time and effort into innovation in the first instance. Patent law solves this problem by granting an inventor a limited monopoly on his or her invention, giving the inventor the prospect of recovering his or her costs and making a profit. The additional potential for profit incentivizes greater innovation in the first instance.

That is the standard patent law story. But in the late 1990s and early 2000s, a growing number of advanced technology firms and industries began to see patent law as flawed and failing to meet its central objective of promoting innovation. Rather than perceiving a patent as providing an incentive to innovate, some began to believe that patents were creating a drag on innovation. Among the most concerned entities were large software and information technology companies who believed that patent law had run fundamentally off-track, to the detriment of innovation in their industries. Many new technology devices, such as a computer, cell phone, or software program, incorporate a vast array of technological advances. A personal computer, for example, contains technology that is the subject matter of thousands of active patents. As a result, anyone seeking to build a better computer must first license thousands of patents from potentially hundreds of different sources. In addition, patent infringement

is a strict liability offense. If even a small section of code in a multi-million line computer program is held to infringe a patent, whether actually copied from the patented invention or independently discovered, the program owner can be enjoined from distributing the entire program and liable for various damages. Add to this the uncertain scope of many patents, due to the difficulty of defining particular technology, and many companies felt they were facing a perfect storm; extraordinarily expensive up-front licensing costs and untoward risk of future patent infringement litigation.

These costs and risks were a dominant force behind initial patent reform efforts that began in 2005. The bill introduced in Congress that year (H.R. 2795, 109th Cong. (2005)) included sweeping changes to patent law designed to make it harder to acquire patents, easier to attack existing patents, and limiting damages and remedies available for patent infringement. The Patent Act of 2005 was met with stiff opposition from a number of industries outside the computer and information fields, particularly the pharmaceutical and biotechnology sectors, who feared that the proposed reforms would wreak havoc on innovation in their industries.

Different Law for Different Industries

Debates over the Patent Act of 2005, subsequent legislative proposals, and concurrent litigation made clear that different industries experience the patent system in

widely different manners. Although American patent law presents a largely uniform body of law across all technologies, the law is experienced differently by different industries. Like the parable of the blind men and the elephant, where each man perceives a different object because each touches a different part of the elephant's body, patent law is perceived differently by different industries because variation in underlying technology characteristics cause different industries to interact with the patent system in different ways.

Pharmaceutical and biotechnological innovation, for example, requires time-consuming, costly, and risky research and development in order to achieve new innovation, such as new drugs and new biologics. Developing a new drug or biologic routinely takes a decade or more, costs hundreds of millions or billions of dollars, and often requires testing hundreds of alternatives or compounds. Technological lifecycles (the length of time before a technology is rendered obsolete by later technological advance) in these fields can measure decades. The software and information technology fields, on the other hand, are less research intensive. New software applications can be produced on much shorter time scales and for a much more limited investment, often under a million dollars. Further, these computer-related fields evolve very quickly, with technological turnover on the order of several years or less. New innovation in these industries quickly becomes obsolete.

Industries also vary into how their technologies interact with the patent system. Pharmaceutical and biotechnological inventions often involve discrete, stand-alone innovation, such as a new drug or new device. These types of inventions are usually relatively easy to reverse engineer and copy. As a result of the ease of duplication and other factors, inventors in these fields have relatively limited means to recover the cost or value of innovation outside of intellectual property protection. Software and information technology innovation, on the other hand, routinely involve cumulative, rather than discrete, advances that evolve independently from one innovation to the next. Cumulative

innovation means that each new invention needs to incorporate a variety of prior patented technology in order to function. In addition, these fields often can rely on methods outside of the patent system in order to profit from their innovation, such as being able to commercialize an invention while maintaining its secrecy, lead-time, or bundling innovation with other sales and services.

Because of the vast differences in the technologies covered by the patent system, patent law plays out very differently for different firms. The same patent law that may be critical to promote pharmaceutical innovation can simultaneously be a costly anathema for many computer-related firms.

The crosscurrents of opposed powerful industry groups led to a stalemate on patent reform efforts in 2005. New patent reform legislation has been introduced in each session of Congress since that time, and each year the proposed legislation has been successively watered down from prior efforts in an attempt to reduce opposition to the bill and increase the chance of passage. In addition, since 2005 the Supreme Court has issued several high-profile patent decisions that either judicially implemented certain elements of the originally proposed reforms or otherwise had the tendency to weaken the strength of patent rights. *See, e.g., eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388 (2006); *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398 (2007). These cases resolve certain of the problems that some industries perceived with the patent system, and reduced the areas of conflict, generating optimism that 2011 may finally be the year patent reform is enacted.

The America Invents Act of 2011

Despite being limited in scope in relation to earlier patent reform bills, the America Invents Act of 2011 incorporates several significant changes to the patent system. These changes include shifting the United States from a first-to-invent patent system to a first-inventor-to-file system, introducing a new way for third parties to challenge patent grants, modifying the role that courts play in the calculation of patent

damages, and effectively prohibiting the patenting of tax methods. Each of these changes is discussed in turn. The act also makes a number of other, more modest, changes to the patent statute.

First-Inventor-to-File

The United States is currently the only country that has a first-to-invent patent system. Under this system, the first inventor to achieve an invention is entitled to a patent on the invention, even if the first inventor is not the first inventor to actually file a patent application on the given subject matter. The rest of the world operates under a first-inventor-to-file patent system; the first inventor to file a patent application, even if he or she was not the first inventor temporally, is entitled to the patent. It bears emphasizing that both first-to-invent and first-inventor-to-file systems only permit patents to issue to actual inventors; if someone derives an invention from another, whether through direct copying or otherwise, she or he is not entitled to a patent, regardless of whether her or his application is filed first. The first-inventor-to-file versus first-to-invent issue only concerns the assignment of patent rights when two inventors each independently achieve the same invention.

The common critique of the first-inventor-to-file system is that it produces a race to the patent office. Consequently, those with greater resources may have an unfair advantage, even if they are not the first to actually invent. In addition, a first-inventor-to-file system can create incentives to file rushed and sloppily drafted patent applications on not-yet-fully developed inventions. Many individual inventors and small entities are opposed to the first-inventor-to-file provisions, out of concern that the change will be advantageous to larger, better funded entities who can prepare their patent applications faster and who may flood the United States Patent and Trademark Office (USPTO) with patent applications.

The great advantages of the first-inventor-to-file system are certainty and the ease of administrability. Under the United States' current first-to-invent system, when two inventors file patent

applications on the same subject matter within a year of each other, the USPTO will declare an “interference.” Interferences are adversarial proceedings that can be both lengthy and expensive. This expense raises some question about small entities’ expectation that they are better off under the first-to-invent system. Finally, an added benefit of switching to a first-inventor-to-file system is that it would harmonize the United States’ patent system with the rest of the world, creating more uniformity in patent applications and practice. Harmonization and eliminating interference proceedings would likely reduce the cost of the patent system, and the resources saved could be devoted instead to further innovation.

The patent bill that passed the House of Representatives (H.R. 1249, 112th Cong. (2011)), but not the bill that passed the Senate, includes a provision that creates a twist on the traditional first-inventor-to-file system. Under the House bill, an inventor who is first to invent (but not first to file) could be entitled to prior use rights. Prior use rights would provide a defense to infringement for an actual first inventor who commercially used an invention that he or she reduced to practice at least one year before the second inventor filed a patent application on the same subject matter. In other words, prior use rights do not prevent a second inventor from obtaining a patent, but can provide a defense to a patent infringement lawsuit.

New Means to Challenge Patent Validity

The America Invents Act includes a couple of new provisions that make it easier to challenge patent applications and the validity of issued patents. First, the proposed legislation allows third parties to submit certain published information relating to a pending patent application for the patent examiner to consider. Second, the proposed legislation increases the opportunity for third parties to challenge the validity of a patent after the patent issues.

Patent law currently provides certain post-grant patent challenge opportunities, but such provisions have been critiqued as not sufficiently effective or efficient. The new provisions create a new opportunity

for post-grant review and modify an existing one. The new post-grant review allows a third party nine months to contest the validity of an issued patent on a variety of grounds. After the post-grant review period, a third party will still be able to challenge a patent, but only on more limited grounds. The precise extent of these grounds varies between the current House and Senate bills, but in each case is more extensive than current law.

Damage Calculations

Damage calculations in patent cases present notoriously difficult challenges. It is often extremely difficult to assess how a competitor’s sales may have been impacted by an infringing device or what proportion of sales or sale price were due to an infringing component of a larger product. The damage provisions of the patent reform legislation considered by Congress have presented some of the most contentious issues, and are likely the reason that certain earlier iterations of patent reform legislation were not enacted.

The current reform bills allow for a gate-keeping role for judges in overseeing the legal basis for specific theories of damages due to patent infringement, as well as overseeing jury instruction concerning damages. In an effort to secure passage, clearer restrictions on potential damages available for infringement have been removed from the legislation.

Prohibiting Tax Patents

In the well-known case of *State Street Bank v. Signature Financial Group* (149 F.3d 1368 (Fed. Cir. 1998)), the Federal Circuit held that patents on methods of doing business were eligible for patent protection just as any other innovation would be. Although framed as a clarification of existing law, this decision led to a raft of business method patent applications and grants, eventually including patents on various tax methods and strategies.

Many tax attorneys and other tax professionals have been outraged by the prospect of tax method patents, creating a situation in which tax professionals could be barred from implementing certain tax planning methods absent licensing a tax

patent from the patent owner. Tax professionals have made several efforts at congressional reversal of the *State Street Bank* decision as it pertains to tax methods. Though they have been unsuccessful in implementing such a change in a stand-alone bill, this year they have managed to work their proposed prohibition on tax method patenting into the broader patent reform legislation.

Both the Senate and House bills include provisions that render ineffectual patents on tax strategies, defined as methods for reducing, avoiding, or deferring tax liability. The House bill has additional language that would also effectively ban the patenting of financial management software.

Slightly Weaker Patents

Taken together, the provisions of the America Invents Act would tend to make it slightly more difficult to obtain a patent in the first instance and slightly easier to invalidate a patent after it has issued. These changes, however, are far less significant than various patent reforms that have been proposed over the past six years. Most large patenting industries now either support or are not opposed to the current proposal. The primary opposition comes from small companies and individual inventors, although other provisions have been added to the America Invents Act in an effort to assuage these concerns or at least to provide some beneficial trade-offs in an attempt to balance the provisions that are perceived as problematic. For instance, recent additions to the act would reduce the patent filing fees for certain small and micro-entities. Any effect on innovation by small entities, such as new start-up companies, is a significant concern because some research indicates that smaller companies are more likely to produce significant innovation than larger companies.

In the end, the America Invents Act, if enacted, can be expected to have only modest effects on research and development and innovation activity in most industries. It will likely slightly reduce the amount and expense of patent litigation, permitting more resources to be devoted to innovation. The biggest effects may

be felt by certain patent practitioners. Interference proceedings for example, a notable area of current practice, will cease to exist. The invention derivation proceedings that will replace them in certain instances will be far less numerous. Similarly, the limited tax patenting industry will also dry up. These impacts, however, are likely a relatively limited cost to bear for a bill that many believe will promote innovation across a wide variety of technology industries.

Gregory N. Mandel is the Peter J. Liacouras Professor of Law and associate dean for research at Temple Law School.

BUSINESS LAW TODAY

The ABA Business Law Section's Online Resource

Speaking Volumes

A Review of *The Subprime Virus:*

Reckless Credit, Regulatory Failure, and Next Steps

By Kathleen C. Engel and Patricia A. McCoy; Oxford University Press

2011; 368 pages; \$34.95 (hardcover list price)

ISBN: 9780195388824

Reviewed by Dwight Golann

Imagine that the *New Yorker* magazine published a series of articles about the subprime lending crisis and its impact on the financial system. It did so in depth, beginning with a boarded-up block in Cleveland and going on to describe how a boom in housing led to bad loans which spread through the system, infecting our largest financial institutions and regulators. The authors wrote in engaging *New Yorker* style, with many fascinating details (did you know that Alan Greenspan invited Ayn Rand to attend his swearing-in as Chairman of the Fed?) The articles would include lucid explanations of complex events, with endnotes to tie everything down. And, of course, the series would have a point of view, in this case that of a consumer activist—but the kind of activist who meticulously confirms facts and understands issues. You would then have *The Subprime Virus* (Oxford University Press, 2011), written by Professors Kathleen Engel and Patricia McCoy.

It is the kind of book Elizabeth Warren might have written if she were not so busy regulating. It shares the perspective of the late Federal Reserve Governor Edward Gramlich's book *Subprime Mortgages: America's Latest Boom and Bust*, although Gramlich did not anticipate a crisis of the entire financial system.

What is the relevance of *The Subprime*

Virus to a business lawyer? Unlike other works which focus on a single aspect of the crisis, this book examines the entire business of marketing and securitizing home mortgages. It shows how mortgage companies and banks began to ignore risk, as executives disregarded what one hopes was cautionary advice from their lawyers. It also analyzes the collapse of federal bank regulation, describing in acerbic tones how regulators, with the notable exception of the FDIC, competed for lender fees by decimating their oversight systems and shielding banks from state regulatory efforts.

Many excellent books on the bubble and ensuing crisis have appeared. Some are entertaining, like Michael Lewis' *The Big Short* and Gregory Zuckerman's *The Greatest Trade Ever*. Those books describe individuals who outsmart the system by buying up swaps and waiting for the bubble to collapse. The traders are anxious and so are we: As they keep renewing their wagers, why don't prices fall? And will the "house"—AIG and other institutions—be able to pay off winning bets?

Others, including Gretchen Morgenson and Joshua Rosner's *Reckless Endangerment: How Outsized Ambition, Greed, and Corruption Led to Economic Armageddon* (2011), focus on the errors and greed of single players such as Fannie

and Freddie, or, like Robert Shiller's *The Subprime Solution: How Today's Global Financial Crisis Happened and What to Do About It* (2008), give an academic assessment of events, with recommendations for the future. There are more than a dozen similar works.

It was to *The Subprime Virus*, however, that the American College of Consumer Financial Services Lawyers gave its book award, most likely because of this book's unique combination of detail, coverage, and style. This may be the only book that looks at the entire business of residential lending, financial regulation, and corrective legislation. It includes capsule accounts of how individual institutions—WaMu, Lehman, and numerous subprime lenders, among others—lost their way. The authors explain why the experts were so wrong—quants, for example, used wonderfully sophisticated mathematical techniques, but failed to include in their models the possibility that housing prices would ever go down. Engel and McCoy provide a stream of intriguing details: for example, toward the end a full 90 percent of all outstanding swaps were naked—bought by people with no ownership stake in the assets they were insuring.

The Subprime Virus does have strengths and weaknesses. A strength is that it is short—only 250 pages exclusive of end-

notes and bibliography. If you, like me, have trouble getting through long works of nonfiction, the brevity and engaging style of this one is a blessing. Occasional anecdotes and cartoons also provide welcome breaks from large doses of facts. As noted *The Subprime Virus* is comprehensive, covering business problems, regulatory reactions, and legislative responses such as TARP and Dodd-Frank. The book is also well-organized; one can read about the real estate and securities aspects of the crisis without going deeply into governmental actions and vice versa.

Weaknesses include: It is not novelistic—the authors must give up the chance to focus on individual heroes or villains. For that I recommend *The Greatest Trade Ever*, describing John Paulson's multi-billion dollar coup in the swaps market. Also, while *The Subprime Virus* describes the passage of Dodd-Frank, it could not

cover the continuing regulatory aftermath. For an account of the fight over the Consumer Financial Protection Bureau, the regulation of derivatives, bank fees, and other topics, we must await books yet to be written.

Finally, the authors are unapologetically pro-consumer, and vehemently critical of now-departed CEOs and regulators. Twenty years ago the Section's Consumer Financial Services Committee decided that to give their clients the best possible advice, it was necessary for business lawyers to listen to the voices of consumer activists—at least the informed ones—and created a Consumer Fellows program. If books could be given such fellowships, this work would receive one.

Carmen Reinhart and Kenneth Rogoff's book *This Time Is Different* reminded us that investment bubbles have occurred regularly throughout human history. *The*

Subprime Virus includes comments and facts which are sometimes hard to listen to, but necessary if we are to help clients prosper, navigate changing regulation, and avoid being consumed by the next, inevitable bubble.

Dwight Golann is a professor at Suffolk University Law School in Boston, where he teaches consumer law, negotiation, and mediation. He is a former chair of the Consumer Financial Services Committee and the Consumer Advisory Council to the Governors of the Federal Reserve.