TRENDS®

YOUR BUSINESS AND THE LAW

MARCH/APRIL 2008

FAEGRE & BENSON LLP

WWW.FAEGRE.COM

UNITED STATES | ENGLAND | GERMANY | CHINA

TRENDS® is published bimonthly by the law firm of Faegre & Benson LLP. Further details are necessary for a complete understanding of the subjects covered by this magazine. For that reason, the specific advice of legal counsel is recommended before acting on any matter discussed on these pages.

For the latest legal news, or copies of any article in this magazine, visit Faegre & Benson online at www.faegre.com. For address and other changes, contact info@faegre.com.

Clean Rooms Are not Just for Kids: How to Demonstrate Independent Development to Avoid a Trade Secret

By Randall E. Kahnke and Kerry L. Bundy

Randy Kahnke, a partner in Faegre & Benson's Minneapolis office, focuses his practice on complex commercial and intellectual property litigation. His email address is rkahnke@faegre.com. Kerry Bundy, a partner in Faegre and Benson's Minneapolis office, focuses her practice on trade secret litigation and counseling, and franchise and distribution law. Her email address is kbundy@faegre.com.

Your company has been sued for trade secret misappropriation. Can you win? One way to avoid liability is to demonstrate that your company used a "clean room" process to independently develop the information at issue. A recent case highlights the importance of knowing when and how to use a clean room.

A $21 Million Jury Verdict Against Sears

Roto Zip, a family-owned tooling company, showed national retailer Sears, Roebuck and Co. its next-generation product, a combination power tool, with the hope that Sears would want to sell it under the retailer's private label. After the parties executed a non-disclosure agreement, Roto Zip shared with Sears its prototypes, exhibits and a proposed marketing plan. Discussions between the two companies broke down, however, over pricing issues. Two years later, Sears introduced a combination tool that Roto Zip claimed was the very same next-generation product it had shown to Sears in confidence. Roto Zip sued Sears in Illinois federal court, alleging that Sears had misappropriated Roto Zip's trade secrets. Roto Zip established that the idea at issue was a trade secret; Sears was unable to demonstrate that it (or one of its affiliates or suppliers) had independently developed the idea. In November 2007, Roto Zip obtained a $21 million jury award—including $8 million in punitive damages.

The Source of Trade Secret Protection: State Law

The Sears case offers lessons both for those seeking to develop a new product that closely resembles a competitor's offering as well as those who believe someone may have stolen their trade secrets.

Trade secret protection emanates from state law—either through the Uniform Trade Secret Act (UTSA), which codifies common law trade secret principles and has been adopted in 45 states, or under the *Restatement 3d of Unfair Competition*, which recognizes substantially similar legal principles.

In order to demonstrate the existence of a trade secret, an individual or company must show two things: First, he or it possesses knowledge or information that is valuable precisely because it is not generally known or readily ascertainable; and second, that the individual or company has made reasonable efforts to maintain the secrecy of the knowledge or information. The UTSA prohibits "misappropriation" of trade secrets, which is generally defined as the use or disclosure of another person's or

company's secret information by someone who knew or should have known that the information was meant to be held in confidence.

A big advantage of trade secret law is that, unlike patents and copyrights, it offers indefinite future protection to the trade secret holder, so long as the information remains secret. In contrast, unlike patents and copyrights, trade secret protection does not grant a trade secret owner exclusive rights to the secret. If a competitor develops a product or information without relying on another's trade secrets, through "reverse engineering" or "independent development," there is no misappropriation of trade secrets.

Consequently, a common fact pattern in trade secret litigation entails a defendant company claiming to have independently developed a product substantially similar to that of the plaintiff trade secret owner, even though the defendant company was exposed to alleged trade secrets—either through a former employee, joint venture, licensing negotiations or submissions by an inventor (as in the Sears case). The case then turns on whether the defendant company can show that its development process was uncontaminated by improperly acquired confidential information. In other words, was the product a result of illegal misappropriation or legal "clean room" development?

Whether a company wants to establish a clean room to defend against a claim of misappropriation, or wants to attack an alleged independent-development effort of a competitor it believes has stolen its trade secrets, the following factors should be considered.

One Approach To Clean Rooms: Three Independent Groups

Clean rooms generally consist of three teams—specification, design and coordination.

- The ***specification team*** analyzes the competitor's product or service and identifies the general parameters for the potential new product or service, creating a list of specifications for developing it. Specifications should not include any reference to the competitor's trade secrets or confidential materials.

Though members of the specification team typically are familiar with the competitor's product, opinions differ on whether the team should ever include individuals who have been exposed to the competitor's confidential information. Some experts believe that as long as the design team is not given trade secrets or copyrighted material, and the specifications do not give the design team tainted clues, then the makeup of the specification team is inconsequential. Others feel it is too difficult to develop specifications free of trade secret or copyright violations when team members have specific knowledge of protected items.

Specification teams should consider keeping all materials used, including sources and dates. Such documents may be valuable later as evidence of what the specification team had access to and provided to the design team.

- The ***design team*** is isolated in the "clean room"—which can be either a separate physical facility or a metaphor for a process that is untainted by access to a competitor's trade secrets. The design team is allowed to access only the specifications and information approved by the coordination team (described below). The design team executes the actual design and development of the product or service.

Members of the typical design team are independent and should be screened to ensure they have had no access to alleged trade secrets. Even the perception of possible knowledge may create complicated issues of fact that need to be resolved later, during litigation. As a cautionary measure, it may even be prudent to limit the design team to engineers who have never worked for the competitor or any company that has had access to sensitive information.

At the same time, the design team must have the credentials and ability to adequately carry out the design. Exceptional credentials may also lend credibility to the clean room process if it is later reviewed by a court.

- The ***coordination team*** serves as a filter or "screen" of the information provided to the design team. The coordination team often evaluates specifications to keep out protected information, screens information that flows in and out of the clean room, and ensures that all procedures are properly followed and documented.

The composition and function of the coordination team will depend on the company, the project at issue, and the likelihood that the company's actions will be scrutinized in litigation. Regarding staffing, it may be beneficial for the coordination team to have members who are competent in both engineering and trade secret law. Engineers can help assure that specifications make sense to designers and spot problems they are likely to face. From a legal perspective, the specifications and other information should not contain any trade secrets or confidential information. If litigation is already underway when a clean room operation is formed, a company may want to have independent engineers and attorneys on the coordination team.

Other Factors to Consider

The Danger of Patents. Although trade secret law cannot protect against the independent development of particular information and ideas, patent law can prevent the duplication of products that are already protected. In other words, the clean room development process cannot circumvent an existing patent. Where circumstances allow, the coordination team will want to research any patents that may apply to the product being developed before the company devotes resources to a clean room process.

Minimalist Specifications. The specification team's list of specs is often the most important source of information for the design team. In general, the specification team should provide the least amount of information that is consistent with an effective approach to the design.

Neutral Product Design Tools. The coordination team may also need to monitor what tools are provided to the design team, as certain tools may force the design in a particular direction. "Tools" can encompass a wide range of instruments, including specific engineering devices and computer software. One option is to make only neutral tools available. Another alternative is to have a wide variety of tools available and provide them only as requested.

Controlled Communication. Communication into and out of the clean room should be controlled and monitored. One approach is to make sure all information is in writing, logged, and kept by the coordination team. Similarly, the coordination team may want to preserve all email communications, to avoid suspicion that information is being passed improperly.

Documenting the Design Process. Documenting the clean room design process can help ensure that the design team followed appropriate procedures and did not have access to improper information. One option involves each design team member maintaining a lab notebook. The coordination team may also create a process for recording the status of the project, including day-to-day activities, diagrams and specifications, at regular intervals. In appropriate circumstances, the design team may want to document both successes and failures, thus helping to show that the final product or service was developed through independent trial and error.

An Objective Termination Point. In setting up the clean room, the company may want to pre-define a termination point. Objective, defined goals for the clean-room project are generally preferred over subjective goals that are more difficult to

evaluate and enforce. Failure to commit to a termination point could lead to the continuous rejection of products developed by the design team. A competitor may then argue that the company rejected products until the design team happened upon the correct result.

Review and Evaluation of Product Design. Another consideration is limiting external review and evaluation of the product designed in the clean room before the end of the clean room development process. As the design team develops preliminary versions of the new product, feedback should be carefully scrutinized to ensure that it is not overtly leading and does not infringe upon the competitor's trade secrets.

Cost-Benefit Analysis. It is important for a company to evaluate the costs and benefits of undertaking a clean room development project, since it is usually an expensive task. Before starting out, evaluate the costs of a clean room compared to the benefits that it can provide.

Conclusion

Innovation can be the lifeblood of a company. As the Sears case demonstrates, however, the negative effects of not following a proper design process can be substantial. Clean rooms offer one way of ensuring that your company's innovation efforts add to, rather than subtract from, your company's growth strategy. FB

Supreme Court Rejects Broad "Scheme Liability" for Federal Securities Fraud

By Martin S. Chester

Marty Chester is an associate in Faegre & Benson's litigation practice in Minneapolis. His practice focuses on securities, trade secret and real estate litigation. His email address is mchester@faegre.com.

On January 15, 2008, the U.S. Supreme Court decided *Stoneridge Investment Partners v. Scientific-Atlanta*. This decision is a major case for publicly held firms and for businesses dealing with them, because it gives some guidance about which members of an alleged fraudulent scheme may be held liable for violating federal securities laws. In a 5-3 decision, the court held that "secondary actors" (such as investment banks, vendors and law firms) that help publicly held companies commit securities fraud cannot themselves be held liable in a civil suit under federal securities laws unless investors actually rely on the secondary parties' actions or statements when making investment decisions.

Why the Supreme Court Addressed This Issue

Stoneridge came to the Supreme Court against a backdrop of cases like those related to the Enron collapse, in which shareholders are often unable to collect money judgments from publicly held companies that committed fraud, because

such companies are often bankrupt. Therefore, many plaintiffs have sued banks, accountants and other entities that allegedly enabled those public companies to defraud their shareholders.

The specific legal issue in *Stoneridge* was whether the Supreme Court should interpret Section 10(b) of the Securities Exchange Act of 1934 and its key regulation, Rule 10b-5, to include liability for such secondary actors. Section 10(b) makes it illegal for any individual to employ "any manipulative or deceptive device or contrivance" in violation of Securities and Exchange Commission rules "in connection with the purchase or sale of any security." Rule 10b-5 prohibits several specific things in connection with the purchase or sale of any security: material misstatements and omissions; employing a scheme to defraud; and engaging in any act or course of business that operates as a fraud.

Until 1994, some lower federal courts allowed private litigants to sue secondary actors for "aiding and abetting" securities fraud when the actors' conduct itself may not have violated Section 10(b), but helped others violate the law. But that year, in *Central Bank of Denver v. First Interstate Bank of Denver*, the Supreme Court held that private parties could not bring suits for aiding and abetting securities fraud. *Central Bank* held that to be liable for securities fraud, a person must have actually committed one of the acts prohibited by the text of Section 10(b). This decision significantly limited securities fraud liability for secondary actors. After *Central Bank*, various federal courts of appeals disagreed about when a secondary actor actually committed securities fraud and was thereby liable under Section 10(b), rather than merely aiding and abetting such fraud, which yields no liability under Section 10(b).

The Facts of the Case

Stoneridge involved a cable television company, Charter Communications, which engaged in a sham accounting scheme involving two of its vendors, Scientific-Atlanta and Motorola. Under the scheme, which was designed to allow Charter to meet Wall Street expectations for subscriber growth and cash flow, the vendors increased the price of cable boxes that they sold to Charter, and then used the additional revenue to buy advertising on Charter's television stations at inflated prices. The vendors were thus "purchasing" advertising with Charter's own money. The vendors facilitated the fraud by, among other things, backdating sales agreements for the cable boxes so that the cable box sales and advertising purchases appeared to be unrelated. These sham transactions enabled Charter to falsely report its financial condition in Securities and Exchange Commission filings.

This scheme was just part of a larger fraud by Charter, which led to criminal charges against its executives and a civil suit by Stoneridge (an investor in Charter). The investors also sued the vendors Scientific-Atlanta and Motorola, alleging that the fraudulent scheme could not have occurred without the vendors' participation.

The trial court dismissed the investors' claims against the vendors, and the U.S. Court of Appeals for the 8th Circuit upheld this ruling. The 8th Circuit held that because the vendors did not actually "speak to the market" by making any fraudulent misstatements or omissions regarding Charter's stock, and because they did not engage in manipulative transactions in Charter's stock, the vendors could not be guilty of anything more than aiding and abetting Charter's fraudulent scheme. And since *Central Bank* prohibited civil liability for aiding and abetting Section 10(b) violations, the 8th Circuit affirmed the dismissal of the investors' claims against Charter's vendors.

The Supreme Court's Ruling

The Supreme Court's decision to review *Stoneridge* was seen as an effort to resolve the split between federal appellate courts agreeing with the 8th Circuit that a party must actually "speak to the market" regarding fraudulent activity to be liable under Section 10(b), and other courts holding

that a secondary actor's mere participation in a "scheme to defraud" is sufficient for civil liability under Section 10(b), even if the secondary actor never communicated with the investing public. While the Supreme Court's ultimate ruling was against the investors, it did not adopt the 8th Circuit's ruling that a secondary actor who does not "speak to the market" cannot be liable under Section 10(b). Instead, the Supreme Court observed that a secondary actor's conduct, not just its statements, can give rise to liability under Section 10(b). Despite this departure from the 8th Circuit's ruling, however, the Supreme Court still held that the conduct of Charter's vendors was not sufficient to impose liability.

The Supreme Court's decision, written by Justice Anthony Kennedy, turned on the concept of the investors' "reliance" on the vendors' deceptive acts. Reliance is a requirement for liability under Section 10(b). The investors, invoking a theory called "scheme liability," argued that even though the vendors did not make public statements about Charter or its stock, their actions allowed Charter to issue fraudulent financial statements, which in turn affected its stock price. As a result, the investors claimed, their purchase or sale of Charter stock at artificially influenced prices meant that they "relied" on the vendors' deception.

The court's majority found this chain of events to be "too remote for liability." The court stated that Section 10(b) liability "does not reach all commercial transactions that are fraudulent and affect the price of a security in some attenuated way." Instead, the court found that because no member of the investing public knew about the vendors' deceptive transactions, the investors could not have relied upon them. The court also held that the vendors owed no duties to Charter's investors, so they were not required to disclose the sham transactions to the investors.

The court held that at most, the vendors might be liable for aiding and abetting Charter's securities fraud, but under *Central Bank*, that is not a valid basis for a claim under Section 10(b). The court noted, however, that parties who aid and abet securities fraud are subject to criminal penalties and civil enforcement by the SEC.

Justice John Paul Stevens dissented, stating that the vendors in *Stoneridge* did not simply aid and abet Charter's fraud, but actually committed fraudulent acts that violated Section 10(b). Justice Stevens, joined by Justices David Souter and Ruth Bader Ginsburg, argued that the vendors could therefore be sued under Section 10(b).

Assessing the *Stoneridge* Decision

The Supreme Court's *Stoneridge* decision has been widely interpreted as a defeat for the plaintiffs' class action bar, which might have used a decision in favor of the investors to pursue many new lawsuits against a vast array of businesses that might arguably be connected to fraudulent schemes of publicly held companies. Indeed, the majority noted that it was concerned about establishing a rule that could "allow plaintiffs with weak claims to extort settlements from innocent companies," and that adopting the investors' proposed "scheme liability" theory for Section 10(b) violations "would expose a new class of defendants to these risks." According to the majority, such a rule would raise the cost of doing business for American companies, and might deter overseas companies from doing business in the United States and thereby shift money away from U.S. markets.

Stoneridge is certainly a positive decision for businesses seeking some measure of comfort that they will not be subject to Section 10(b) liability for engaging in legitimate transactions with a publicly held company that later uses those transactions to commit securities fraud. Indeed, *Stoneridge* is the latest in a series of recent cases demonstrating that a majority of justices are opposed to further judicial expansion of Section 10(b) liability. Further evidence is the Supreme Court's refusal—shortly after issuing the *Stoneridge* decision—to review

another scheme liability case (involving Enron) in which the plaintiffs made claims similar to those brought by the *Stoneridge* investors.

Nevertheless, as one SEC commissioner has noted, it would be a mistake to see *Stoneridge* as a "free pass" to companies committing fraudulent acts. First, although parties that aid and abet securities fraud are not subject to Section 10(b) liability, they can be punished by the SEC. Moreover, by rejecting the 8th Circuit's standard for liability under Section 10(b), the Supreme Court appeared to recognize that some conduct by "secondary actors" (i.e., firms that are not the publicly held company making false financial disclosures) could be relied upon by investors, thereby converting the "secondary" actors to primary violators of Section 10(b). The precise nature of what conduct may be relied upon by investors will likely be clarified in future cases, but this seems to be a surviving avenue for liability after *Stoneridge*, and is yet another reason for companies to be scrupulous in making sure that all their business dealings are legitimate and proper. FB

Minnesota's New "Plastic Card Security Act": A Harbinger of Things to Come?

By Michael P. Carlson and Laura E. Meyer

Mike Carlson is a partner in Faegre & Benson's Minneapolis office whose practice is focused in the areas of financial services regulation and financial privacy. He can be reached at mcarlson@faegre.com. Laura Meyer, a staff attorney at Faegre & Benson, is also based in Minneapolis. She can be reached at lmeyer@faegre.com.

You have seen the news reports or read the newspaper articles: A large company loses the credit information of thousands of its customers. The requisite mea culpa follows, but nonetheless, thousands of consumers have been exposed to the possibility of identity theft or credit card fraud. Indeed, credit card fraud and identity theft are increasing, as are concerns that companies are failing to adequately safeguard customer information. The bottom line is that companies without an appropriate security framework risk significant monetary and reputational losses if their customers' information is stolen. Further, given the ever-growing body of security laws, data breaches have mounting consequences for companies.

The media spotlight on privacy and data security has only intensified in the wake of the massive data breach at TJX Companies (owner of the popular TJ Maxx and Marshalls stores). In that debacle, at least 47.5 million credit card numbers were stolen over a period of several years, in what security specialists have noted is the biggest data breach in history. TJX is facing a federal investigation as well as numerous civil lawsuits from its customers and banks. Eighteen separate lawsuits have been filed against TJX, including two class action suits that seek to hold the company responsible for the losses absorbed by the financial institutions involved. The cost of TJX's internal investigation and installation of new security software has already reached $5 million dollars.

In the spring of 2007, even as the TJX disaster continued to make national news, the state of Minnesota raised the stakes considerably, enacting the nation's first law designed to make merchants liable for their data retention practices. Portions of the so-called "Plastic Card Security Act" took effect in August 2007. The law's liability provisions, which will not take effect until August 1, 2008, essentially impose strict liability on merchants that violate the law's data breach provisions. When those provisions take effect, a company that has customer data stolen and is later found to have stored prohibited data on its computer system will have to reimburse financial institutions for costs, such as blocking credit card numbers and issuing new cards.

But while Minnesota was the first state to pass data liability legislation, it was far from alone in attempting to address the underlying problem. Legislators in at least four of the nation's largest states—California, Illinois, Massachusetts and Texas—considered and in some cases passed similar legislation. The Texas House of Representatives passed its version of a bill 139-0, but the law stalled in the Senate. In California, only Gov. Arnold Schwarzenegger's veto pen prevented AB 779 from becoming law. In his veto message, the Republican governor expressed concern that the bill would "drive up the costs of compliance, particularly for small businesses."

Moreover, because Minnesota's Plastic Card Security Act essentially tracks security standards developed by the financial services industry and used around the world, it is almost certainly a harbinger of things to come across the United States.

Minnesota's Response—Protect Personal Information or Pay the Price

Minnesota's new statute prohibits the retention of "the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction" by any person or entity "conducting business in Minnesota." (The implications of this law for entities without a physical location in Minnesota are not yet clear. While an analysis of jurisdictional issues is beyond the scope of this article, ongoing contacts with Minnesota residents will likely subject persons or entities to this law.)

Minnesota's Plastic Card Security Act essentially tracks the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS was developed by the founding brands of the PCI Security Standards Council (American Express, Discover Financial Services, JCB MasterCard Worldwide and Visa International) to promote the adoption of uniform data security measures worldwide. (Information about the PCI DSS is available at *http://www.pcisecuritystandards.org*.) Requirement 3 of the PCI DSS directs businesses that accept payment cards (credit cards, debit cards, stored value cards, etc.) to minimize cardholder data storage and prohibits storage of the full information of any track from a card's magnetic strip, the card-validation code or value, and the personal identification number (PIN) or encrypted PIN block. The PCI DSS is enforced by the payment card industry, which has in the past fined members for failing to implement and/or adhere to the standards.

In the TJX debacle, for example, Visa U.S.A., Inc. fined Fifth Third Bancorp (the merchant acquirer for TJX Cos., Inc.) at least $880,000 for the massive security breach. This fine included an additional $380,000 fine under Visa's Payment Card Industry Compliance Acceleration Program, which encourages companies to adopt and adhere to the PCI standards. Further, Fifth Third Bancorp could face even more fines. Visa's fines do not begin to address the MasterCard accounts that were also compromised due to the breach.

The Plastic Card Security Act also contains a new provision that essentially imposes

strict liability on merchants that violate the data breach provisions of the new law. (This provision will not become effective until August 1, 2008.) Under the new law, merchants (such as TJ Maxx) will be liable for damages incurred because of a security breach, regardless whether the breach is the result of negligence or faulty security systems. Specifically, the Plastic Card Security Act requires companies to reimburse card-issuing financial institutions for the "costs of reasonable actions" to protect cardholder information as well as provide service to cardholders following a security breach. Card-issuing financial institutions are entitled to recover all costs associated with: (1) the cancellation or re-issuance of any access device impacted by the breach; (2) the closure of any affected accounts; (3) the opening or reopening of any affected accounts; (4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction; and (5) the notification of the cardholders affected by the breach. The new costs imposed by the statute are in *addition* to any other remedy available to the financial institutions.

Minnesota also has a data breach notification law that requires individuals and businesses to disclose security breaches and notify "any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Notably, compliance with this statute could force a merchant to acknowledge potential liability for any costs associated with remedying the security breach. An issuing financial institution is not likely to receive direct notice from a merchant, but it is likely to learn of the notice. A financial institution could therefore try to rely on the merchant's acknowledgement of a security breach in order to recover under the Plastic Card Security Act.

The Domino Effect: Additional State Proposals

Although Minnesota is the first state to pass legislation regarding liability for data security, several other states are considering (or have considered) similar legislation. In May 2007, for example, the Texas House of Representatives unanimously approved a bill that would have required businesses to comply with all PCI DSS requirements. Texas House Bill 3222 would also have allowed a financial institution to bring an action against a business that was subject to a breach of system security if, at the time of the breach, the business did not comply with payment card industry data standards. However, the Texas legislature failed to pass the bill prior to the end of its legislative session.

Although vetoed by Gov. Schwarzenegger, recently proposed legislation in California also attempted to enact stronger data protection requirements as well as provisions allowing reimbursement for costs associated with any security breach. In vetoing the bill, the governor claimed that the costs of such legislation would be excessive for small businesses. What is notable about the proposed California legislation is that it would have permitted any "owner or licensee of personal information" to recover the costs of providing notice to consumers of a security breach.

Similar legislation has been proposed in Illinois and Massachusetts. The proposed Illinois law would impose liability on a data collector for costs incurred by the financial institution in connection with unauthorized use or access to customer accounts or cards. In Massachusetts, the legislation under consideration would also provide for liability to the financial institution for costs associated with a data security breach. While none of these proposals has been enacted, it seems clear that more and more states are looking to tighten the existing legal framework surrounding data security and allocate the costs of a security breach. Financial institutions are also increasing their lobbying efforts to shift the costs associated with a card security breach. They are doing so because under the current legal framework, the allocation of liability falls almost entirely on the financial institution. Both the Gramm-Leach-Bliley Act (GLBA) and the Electronic Funds Transfer Act

Given the contractual and business incentives for card processors to comply with the PCI DSS, some critics question whether Minnesota's law really creates any new incentives for businesses to be more compliant

(EFTA) have provisions requiring the financial institution to carefully safeguard consumer information and assume liability for unauthorized transactions.

In Minnesota, the primary driver of the Plastic Card Security Act was the Minnesota Credit Union Network, which wanted to create incentives for businesses to prevent security breaches. The retail industry strongly opposes such legislative efforts, emphasizing that credit card vendors already impose contractual penalties for failure to comply with proper security measures. In the end, state efforts at legislating data security could prove unnecessary, as Congress seems inclined to address the issue. Bills introduced last year by Sens. Patrick Leahy of Vermont and Dianne Feinstein of California (S. 495 and S. 239), for example, would have required notification for security breaches and authorized actions by a state's attorney general to enforce the violations. Though neither bill passed, Congress may well feel pressure to revisit the issue, especially as state legislatures increasingly seek solutions.

Minnesota's Data Breach Statute Is Not Really Revolutionary

Although the liability provisions of Minnesota's Plastic Card Security Act are new, implementation should for most companies require little in the way of additional effort due to the law's incorporation of what is essentially already required by the PCI DSS. The payment card industry standards long ago mandated the same prohibitions on the retention of security code data. The PCI DSS includes twelve data security requirements that apply to every organization that processes credit or debit card information. (See also the PCI Compliance Guide, available at *http://www.pcicomplianceguide.org*.) Specifically, the PCI DSS mandates that card processors keep cardholder data storage to a minimum by truncating the personal account number of a cardholder and not retaining information such as the personal identification number or the full contents of any track of the magnetic stripe on the back of a card. Companies were required to implement the PCI DSS standards by 2005, though according to one reliable estimate only approximately 18 percent of smaller merchants are compliant. A single violation of the PCI DSS requirements can trigger an overall status of "non-compliance," resulting in fines, suspension and possible revocation of card processing privileges.

Given the contractual and business incentives for card processors to comply with the PCI DSS, some critics question whether Minnesota's law really creates any new incentives for businesses to be more compliant. Clearly, however, companies doing business in Minnesota should review their policies and procedures to limit possible exposure as a result of the new law. Strict compliance with the PCI DSS requirements is essential when handling credit card data. Further, any third-party service provider contracts should be reviewed for compliance. By codifying the standards, Minnesota is unlikely to reduce identity theft but, at the very least, merchant awareness regarding the significance of data security may be increased. FB

NLRB Rules on Employee Use of Company Email for Union Purposes

By John W. Polley

John Polley (jpolley@faegre.com) is a partner at Faegre & Benson. Based in the firm's Minneapolis office, he works extensively in labor-management relations, including collective bargaining negotiations, arbitrations, the defense of unfair labor practice charges, and opposing union organizing campaigns.

Ever since the advent of email in the workplace, employers have sought guidance about whether they may lawfully prohibit employees from using company email systems to solicit other employees to support a union. Since most employers permit employees to use company email for at least some personal communications, the concern has been that prohibiting employee use of email for union solicitations would run afoul of nondiscrimination rules under the National Labor Relations Act, which very generally prohibit limiting employee communications in the workplace about union matters if similar employee communications about other matters are permitted. In *Guard Publishing Company*, a decision released on December 16, 2007, the National Labor Relations Board finally addressed these email issues, albeit in a sharply divided fashion that leaves the outcome of future cases somewhat uncertain.

At the core of the seven-year-old dispute in *Guard Publishing* is a fundamental disagreement about the very nature of email and its role in the modern workplace. The three-member majority, Republicans all, compared email to older, simpler and more tangible communications media, such as bulletin boards and telephones. "[T]he Board," they wrote, "has consistently held that there is 'no statutory right…to use an employer's equipment or media,' as long as the restrictions are nondiscriminatory." The two Democrats sharply delineated the conflict, dissenting in colorful language: "Today's decision confirms that the NLRB has become the 'Rip Van Winkle of administrative agencies.' Only a Board that has been asleep for the past 20 years could fail to recognize that e-mail has revolutionized communication both within and outside the workplace. In 2007, one cannot reasonably contend, as the majority does, that an e-mail system is a piece of communications equipment to be treated just as the law treats bulletin boards, telephones, and pieces of scrap paper."

In *Guard Publishing Company*, the NLRB held that an employer may prohibit employees from using a company-owned email system to solicit for "non-job-related reasons," even if the employer had allowed employees to use the email system for various personal reasons, such as giving away tickets or announcing the birth of a child. However, the *Guard Publishing* decision, in addition to being divided along party lines, came just as the terms of two Board members in the majority (and one in the dissent) were about to expire. There is thus real doubt about whether this decision will remain law when a new, full Board is constituted. There is also some doubt about whether portions of this decision will survive on appeal.

continued on page 16

John Grobowski to Head Faegre & Benson's Shanghai Office

John V. Grobowski

Faegre & Benson LLP is pleased to announce that **John V. Grobowski** has joined the firm as managing partner of its Shanghai office and co-chair of its 15-member China practice. Grobowski joins a legal team that has enjoyed tremendous growth since the opening of Faegre & Benson's Shanghai office in 2001.

Grobowski brings to Faegre & Benson more than 20 years of experience in the China business environment. He will co-chair the firm's China practice with George D. Martin, who founded the practice in 1999 and now divides his time between the Faegre & Benson offices in Minneapolis and Shanghai.

Grobowski joins Faegre & Benson from Baker & McKenzie, where he practiced law for 17 years and served as co-managing partner of the firm's Shanghai office. Currently a governor and the secretary of the American Chamber of Commerce in Shanghai, he has served on advisory panels for government agencies in the People's Republic of China regarding competition law legislation and venture capital law reforms. He is a frequent speaker and writer on numerous aspects of business law in China, and is fluent in Mandarin.

Faegre & Benson's China practice advises U.S., European and Asian clients on cross-border business transactions and dispute resolution matters throughout the Greater China region. Grobowski's practice focuses on advising multinational corporations in the establishment, acquisition and operation of manufacturing companies and service providers throughout China. FB

Faegre & Benson Advises Clients Worldwide on a Trio of AIM Listings

Led by attorneys in the firm's London office, Faegre & Benson has recently helped three companies from around the world gain admission to the Alternative Investment Market (AIM), the 13-year-old sub-market of the London Stock Exchange that has become a premier venue for young, growing companies seeking to raise capital.

In one deal, Faegre & Benson advised Zimmerman Adams International, nomad and broker, and Alexander David Securities Limited, placing agent, in their role as advisers to Armor Designs Inc. (ADI), a Phoenix, Arizona-based maker of protective armor. ADI raised US$16 million. The Faegre & Benson team was led by **Melanie Wadsworth** in London, assisted by **Nicholas Jennings** in London and **Morgan W. Burns** and **Matthew Kuhn** in Minneapolis. **Michael Evans** in London and **Gary S. Weinstein** and **Ed Crouter** in Minneapolis also advised on the intellectual property aspects of the transaction.

In a second transaction, a Faegre & Benson team led by corporate associate **Simon W. Holden**, assisted by associate **Nick Jennings**, represented the joint brokers and nominated adviser to Globo PLC, a leading Greek information technology company. Globo's market capitalization on admission to AIM was more than £26 million.

A third transaction saw the firm's London and Shanghai offices teaming up to assist Natsun Holdings Ltd, a Hong Kong-incorporated fabric and garment producer based in Shandong Province in the People's Republic of China. **Jun George Qi** from the Shanghai office led the transaction, which raised approximately £6.3 million for Natsun Holdings. He was assisted by **Simon Holden** and **Simon C. Hughes** in London and **Yiqiang Li** in Shanghai. FB

Faegre & Benson Attorneys Earn Recognition by *Chambers USA*

Fifty-three Faegre & Benson lawyers have been named "Leaders in their Field" in the 2008 edition of *Chambers USA: America's Leading Lawyers for Business. Chambers USA* is an annual guide that ranks attorneys and law firms based on in-depth research and interviews with clients, attorneys and corporate counsel.

In addition to naming the 53 individuals, *Chambers USA* recognized the firm's depth of capabilities and experience in a number of key practice areas.

In Colorado, the firm was ranked in seven categories: Corporate/M&A, Environment, Intellectual Property, Labor & Employment, General Commercial Litigation, Real Estate, and Construction.

Chambers USA ranked the firm's Minnesota office in Construction, Corporate/M&A, Labor & Employment, General Commercial Litigation, and Real Estate.

Nationwide, Faegre & Benson was ranked in three categories: Franchising, Native American Law, and Privacy & Data Security.

More detailed rankings will be announced with the official publication of *Chambers USA: America's Leading Lawyers* for Business in June. FB

Firm Receives Faculty of Federal Advocates Pro Bono Award

Faegre & Benson received the 2008 Faculty of Federal Advocates Donald E. Cordova Distinguished Service Award at the Rocky Mountain Regional Conference of the American Bankruptcy Institute. The award recognizes excellence in pro bono representation of debtors in federal bankruptcy court, defending against objection to discharge actions filed by creditors.

Darrell M. Daley (Partner, Boulder) accepted the award on behalf of the firm, as he has personally handled or supervised several of these matters over the past few years. Associates **Laura Hutchings**, **Kathy Schaeffer** and **Mary (Mindy) V. Sooter** are also working on referrals from the FFA's Trial Advocacy Training Program. Partner **William J. Leone** (Partner, Denver) on *Minnesota Lawyer* is an instructor in this program. FB

Brian Melendez Named *Minnesota Lawyer* Attorney of the Year for Second Time

Brian Melendez

The legal newspaper *Minnesota Lawyer* has named partner **Brian Melendez** as one of its "Attorneys of the Year" for 2007. The award—now in its ninth year—is reserved for 15 lawyers who distinguish themselves through exemplary work. Also a 2002 recipient of this award, Melendez is just the second lawyer in the state to be honored twice.

Melendez is currently the president of the Minnesota State Bar Association. He also served on the Minnesota Citizens Commission for the Preservation of an Impartial Judiciary, often known as the "Quie Commission." His practice includes arbitration, business and commercial litigation, and numerous areas related to credit and lending. FB

Firm Sponsors Minnesota Lavender Bar Association Annual Conference

Faegre & Benson sponsored the annual conference of the Minnesota Lavender Bar Association (MLBA), held on January 26, 2008, at William Mitchell College of Law in St. Paul. Among the speakers were partner **Brian Melendez**, president of the Minnesota State Bar Association, and Minnesota Supreme Court Associate Justice G. Barry Anderson, who presented on "Judicial Election or Selection in Minnesota: Where to Next?" Their session discussed the Quie Commission's March 2007 report on possible changes to the way Minnesota picks its judges, in light of the U.S. Supreme Court ruling in *Republican Party of Minnesota v. White*.

The MLBA, a recognized affiliate of the Minnesota State Bar Association, works to build community among members through educational programs, networking opportunities, social events and support of student groups at all of Minnesota's law schools. MLBA also works to assure that Minnesota is a community where legal professionals can thrive regardless of sexual orientation, gender identity or HIV status. FB

Thomas Crosby and Richard Duncan Receive Benson Awards for Pro Bono Service

Thomas M. Crosby, Jr.

Faegre & Benson recently named **Thomas M. Crosby, Jr.** and **Richard A. Duncan**, both partners in the Minneapolis office, recipients of the 2007 John C. Benson Pro Bono Award in recognition of their outstanding commitments to pro bono legal service. Along with the honor, each recipient was entitled to designate a community nonprofit organization to receive a $3,000 contribution from Faegre & Benson.

Richard A. Duncan

Crosby, a former chair of the firm's management committee and longtime director of the Faegre & Benson Foundation, was recognized for his leadership role over 42 years with the firm in expanding its capacity to provide pro bono legal representation as well as its leadership-level charitable support of numerous community legal aid organizations. Crosby's work has shaped Faegre & Benson's firm-wide charitable giving policy, strengthened its public service culture and fueled several major pro bono and legal services initiatives to serve low-income clients. He chose the Greater Twin Cities United Way to receive a $3,000 donation from the firm.

Duncan was honored for his contributions to the firm's nationally recognized pro bono environmental and public interest law practice over the past 20 years. In more than 50 matters—including many high-profile cases across the country—he has successfully represented clients in litigation to protect endangered species, migratory birds, wilderness areas and national parks, as well as to advocate for clean air and water, and for the humane treatment of animals. He elected to split the $3,000 donation between the Sierra Club Foundation and the Wilderness Program of the Izaak Walton League of America. FB

Firm Wins Key Appellate Victory for Long-Time Client

Eleasalo V. Ale

Nathaniel J. Zylstra

Faegre & Benson recently achieved a significant victory for long-time client Gabbert and Gabbert Company, the owner of the Galleria Shopping Center in Edina, Minnesota. In the fall of 2005, Gabbert announced plans to build an 18-story luxury Westin hotel and condominium tower next to the Galleria. Barnes & Noble, a Galleria tenant, claimed that the development would violate its lease and sued Gabbert in the summer of 2006, seeking an injunction blocking construction and damages for alleged lost sales. After a week-long bench trial, the trial court dismissed Barnes & Noble's claims, finding that the development did not violate the lease and that, in any event, the court would not grant a permanent injunction. Construction began, with the hotel and condos scheduled to open later this year. Even so, Barnes & Noble appealed, and in February the Minnesota Court of Appeals affirmed the trial court in all respects.

Eleasalo (Salo) V. Ale and **Nathaniel J. Zylstra** handled the trial and appeal, with excellent support from **Robert L. Schnell, Jr.**, **Eileen M. Hunter**, **Charles S. Ferrell**, **D. Charles Macdonald**, **Liz Shields Keating**, **Martin S. Chester**, **Tyler D. Candee**, **Kristin A. Jameson** and **Rachel L. Hetland**. FB

Twenty-Four Faegre & Benson Lawyers Named to Minnesota Rising Stars 2008

Twenty-four Faegre & Benson LLP lawyers are named in the Minnesota Rising Stars 2008 list. Rising Stars must be 40 or younger, or have been practicing law for 10 years or less, and represent the top 2.5 percent of up-and-coming attorneys in the state, as selected through a multi-step peer review and research process. Names were published in the December 2007 issues of *Minnesota Law & Politics*, *Twin Cities Business* and *Mpls. St.Paul Magazine*. FB

Tax Attorney Liane L. Heggy Joins Faegre & Benson

Liane L. Heggy

Faegre & Benson is pleased to announce that Liane L. Heggy has joined the firm's Denver office as special counsel in the corporate practice.

Heggy advises clients on a broad range of corporate, partnership and tax matters, including planning for corporate acquisitions and reorganizations, joint ventures, stock option plans, executive compensation, private equity and hedge fund structuring and operations, and international transactions. She also represents clients in controversies with the Internal Revenue Service and state and local taxing authorities.

She received her J.D. and LL.M. from Georgetown University Law School. Heggy also received B.A., M.A. and Ph.D. degrees from the University of Maryland, College Park. FB

NLRB Rules on Employee Use of Company Email for Union Purposes

Story continued from page 11

Facts of the Case

Guard Publishing Company publishes *The Register-Guard*, a daily newspaper in Eugene, Oregon. About 150 employees working in the newsroom and certain related departments are represented by an affiliate of the Communication Workers of America. Virtually all of those employees used the company's email system at the time this dispute arose in mid-2000. When it installed the email system, the employer had implemented a "communications systems policy," which stated:

> Company communications systems and the equipment used to operate the communication system are owned and provided by the Company to assist in conducting the business of The Register-Guard. Communications systems are not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

Notably, the policy did not prohibit all non-job-related uses of email (or of any other company-owned communication system), and employees had for years used email to communicate with each other about personal matters such as baby announcements, jokes, party invitations, offering sports tickets, organizing poker games and making lunch plans. However, there was no evidence that employees had used the system to solicit other employees for commercial ventures, religious causes or any outside organization.

During protracted collective bargaining, the union's president, who was herself a bargaining-unit employee, used the email system on three occasions in May and August of 2000: (1) to inform employees about an inaccuracy in a prior union email communication about a union rally that had taken place the prior week; (2) to solicit employees to "wear green" in support of the union's bargaining demands; and (3) to solicit employees to march with the union in a local parade to show further solidarity. The first of the emails was sent from the company-owned computer that the employee used at work; the second and third emails were sent from the union's offices, but were addressed to other employees at their *Register-Guard* email addresses. The employer disciplined the union president for each of her three emails, although no solicitation was involved in the first one.

The Board's Ruling

The Board ruled 3-2 that: (1) the employer's communications systems policy was facially lawful; (2) the disciplinary action based on the emails soliciting support for the union's bargaining positions was not unlawful, notwithstanding the fact that the employer had permitted other non-job-related uses of the system; and (3) the disciplinary action based on the informative (i.e., non-soliciting) email was unlawful.

The three Republican members of the Board found the employer's communications systems policy to be lawful. They reasoned that company-owned email systems are no different from company-owned telephone systems, bulletin boards, copiers or televisions. Just as an employer may limit the use of its bulletin boards, the majority held, an employer may limit the use of its email system.

The majority concluded that the employer did not have to justify its email policy, nor modify it to accommodate the Section 7 right of employees to discuss union issues during non-working time. Instead, the Board focused on the fact that the email system is owned by *The Register-Guard*, and its employees had ample opportunities to talk with one another about union issues during non-working time. Thus, just as an

employer who owns its bulletin boards and telephones need not allow employees to use those communications media for non-job-related reasons, *The Register-Guard* was not required to allow employees to use its email system for non-job-related purposes.

The dissent's approach was fundamentally different and would, if adopted by a newly constituted Board, almost certainly dictate a different result. The dissent said email "cyberspace" is akin to the workplace itself or, as the dissent called it, a "natural gathering place." Since that is "where" employees do much of their communicating in the 21st century, the dissent would shift the focus to whether the employer's communications systems policy "interfered" with employees' Section 7 rights to discuss and solicit support for the union while on company property, if it is during non-work time. Since *The Register-Guard*'s communications systems policy did prevent employees from using email to solicit others on union-related matters, the dissent would require the employer to demonstrate legitimate business reasons for such a policy that outweigh the interference. Again equating cyberspace to the actual workplace, the dissent noted that this balancing approach is the one the Supreme Court used more than 60 years ago in approving the Board's long-standing rule that prohibitions against oral solicitations in the workplace during non-working time are presumptively unlawful.

The Board majority also held that the employer's application of its communications systems policy was not unlawfully discriminatory, even though *The Register-Guard* had allowed employees to use the email system for a variety of personal matters. While the Board had, for years, held that an employer may not prohibit union postings on company bulletin boards while allowing personal postings, in its Register-Guard decision the Board overruled that precedent and adopted the reasoning of two 7th U.S. Circuit Court of Appeals decisions holding that unlawful discrimination must reflect "unequal treatment of equals." In *Guard Publishing*,

the Board majority held that "unlawful discrimination consists of disparate treatment of activities or communications of a similar character because of their union or other Section 7-protected status." Noting that there was no evidence that any Register-Guard employee had ever used the email system to solicit on behalf of any kind of group or organization, and that the employer's communications systems policy prohibited non-job-related solicitations, the Board majority concluded there was "no unequal treatment of equals." Also, the majority gave other examples of permissible "line drawing," stating that nothing in the National Labor Relations Act prohibits line-drawing on "non-Section 7" bases such as: charitable solicitations versus non-charitable solicitations; personal solicitations (e.g., selling a car) versus commercial solicitations; invitations for an organization versus invitations of a personal nature; solicitations versus mere talk; and business versus non-business related uses. Notably, the Board cautioned that "if the evidence showed that the employer's motive for the line-drawing was antiunion, then the action would be unlawful."

Applying this new test, the Board majority held that *The Register-Guard* had lawfully disciplined the union's president because of her two emails that solicited other employees to take action (even though those emails originated outside the employer's offices and from one of the union's computers); and had unlawfully disciplined the union's

president as a result of the informational email that had not solicited employees to do anything. The majority noted that the employer's communications systems policy did not prohibit all non-job-related communications, only "non-job-related solicitations."

It seems quite likely that the union will appeal the *Guard Publishing* decision.

Moreover, if a Democrat wins in November's presidential election, there is a significant risk that a Democratic Board would overrule at least some of this decision. Therefore, any employer adopting or modifying its email policies may wish to carefully consider whether it may have to justify to a future Board the business reasons for its policies, or else show that it has not allowed various kinds of personal email. These are issues that should be discussed with counsel. FB

The New Look of Immigration Enforcement: "ICE" Sends a Chill Through Workplaces Across the United States

By Scott W. Wright

Scott Wright is a partner in Faegre & Benson's Minneapolis office, where he handles all aspects of immigration law, including I-9 compliance, audits and employer sanctions. His email address is swright@faegre.com.

The federal agency known as U.S. Immigration and Customs Enforcement (ICE) was established in 2003 as a sub-agency of the newly formed U.S. Department of Homeland Security (DHS). ICE took over responsibility for enforcing immigration law from the disbanded Immigration and Naturalization Service (INS), while U.S. Customs and Border Protection (CBP) and U.S. Citizenship and Immigration Services (USCIS) assumed responsibility for other INS functions. For the first two years of its existence, ICE confined itself mostly to enforcing the law in worksites that involved national security or critical infrastructure. The agency took its first significant steps to prosecute illegal employment in other types of workplaces in 2005.

In 2006, the agency dramatically increased its enforcement efforts, particularly in industries that had long been associated with employing large numbers of illegal aliens. Most significantly, in April ICE simultaneously raided more than 40 pallet plant facilities owned and operated by IFCO Systems North America, arresting nearly 1,200 illegal aliens—and several senior managers. And in December, the agency again staged a series of simultaneous raids, this time at six Swift & Company meat plants spread throughout six states. ICE agents arrested more than 1,200 illegal aliens; of those, approximately 270 were criminally charged for identity theft or the use of fraudulent documents.

These highly orchestrated raids drew nationwide media attention—exactly what ICE leaders intended. The symbolism was stark. ICE was not just the old INS with a new name.

And ICE was just warming up. Bolstered by increased budgets and broad public support, ICE again increased its worksite enforcement activities in 2007. Most of the agency's significant raids and prosecutions were the result of lengthy investigations, dating back a minimum of several months and in some cases years. Those efforts featured an unprecedented level of collaboration with U.S. attorneys' offices across the country, and with a variety of other federal and state law enforcement agencies. As the frequency of ICE's actions in the workplace rose, however, their novelty quickly wore off, and most cases received little media attention outside the metropolitan area where the raid or arrests took place.

Lost in that sporadic and scattered media attention was the fact that ICE's tactics reflected an extraordinary shift in strategy. No longer were those who enforce U.S. immigration laws content, as the INS was, to watch administrative judges impose slap-on-the-wrist fines and send illegal immigrants home. Instead, they have prosecuted a surprisingly high number of company owners, managers, human resources personnel and others in federal court, imposed heavy fines, seized property and bank accounts, and even sent people to prison for immigration-related charges. Yet, these events often failed to resonate in the business community, as other events dominated headlines and priority lists.

The Message for Employers: Make Compliance a Priority

For employers, it's important to realize, among other things, how 2007 was different from 2006, as ICE has shown an ability to adapt and change in its efforts to aggressively curtail illegal employment. Faced with criticism, lawsuits and, in some cases, reluctance on behalf of federal prosecutors, the agency has steered away from high-profile, multi-site raids, targeting a substantial number of small and medium-sized employers, such as restaurants, construction companies and manufacturing plants.

In addition to conducting raids, in 2007 ICE worked to develop a more diversified approach to worksite enforcement. Recognizing the depth of the problem and the sophistication of the illegal employment culture, ICE developed a portfolio of tactics, which included the following:

- ***Increased Worksite Arrests.*** ICE quite simply set out to handcuff more illegal aliens. And succeeded: In 2007, ICE reported making over 4,000 worksite arrests, its highest total ever.
- ***Increases in Fines and Judgments.*** ICE secured immigration-related fines and judgments against employers totaling in the range of $30 million. These fines and judgments were coupled with more than 850 criminal arrests in 2007. All were record highs.
- ***Arrests of and Criminal Charges Against Business Owners, Managers and Human Resources Personnel.*** Across the United States, ICE worked with U.S. attorneys to file criminal charges against the business owners, managers and human resources personnel who illegally hired, employed and sometimes provided shelter for immigrants. Some went to prison.
- ***Targeting of Fugitive Aliens.*** In the past two years, ICE has quadrupled its staffing of Fugitive Operations Teams, which have apprehended tens of thousands of illegal aliens who were criminals or had outstanding deportation orders. Although these efforts do not target employers, the arrests nevertheless affect businesses, as thousands of fugitives and some family members have disappeared from the workforce.

- ***Document and Benefit Fraud Task Forces.*** These two task forces have been working in many of the country's major cities. Task force investigators provide ICE and other law enforcement agencies with leads, which have resulted in the arrest of illegal alien workers across the country. The task forces were credited with developing evidence that led to 1,500 arrests in 2007. In some cases, ICE and other agencies arrested individuals who provide illegal immigrants with fraudulent documents. In others, they filed charges against workers.

- ***Partnerships with Local Law Enforcement Agencies.*** ICE has two programs through which its agents work with and train both state and local law enforcement officers. The "ICE ACCESS" program focuses on fighting traditional criminal activity. The second program, called "287(g)" (the name of the law that authorizes its funding), provides state and local officers with training to combat identity theft and illegal immigration. In 2007, ICE provided training to 33 different local law enforcement agencies. The agency refers to these programs as a "force multiplier"—an accurate description, as local agencies put their training to use in a number of worksite-related initiatives that targeted illegal immigrants in 2007.

Other Enforcement Trends

Today interagency cooperation is the norm when it comes to enforcing immigration law, not the exception. It's not uncommon for a half dozen or more local, state and federal agencies to work together on an investigation—the Social Security Administration, state wage and labor investigators, postal service investigators, the U.S. Department of Labor and others. In some cases, state and local law enforcement agencies, sometimes—but not always—trained by ICE, have taken the lead in investigating alleged violations. This trend is almost certain to grow in the next few years, as numerous states follow the lead of Arizona, Colorado and others, enacting immigration laws and policies of their own.

Meanwhile, ICE has expanded its geographic reach, targeting businesses in parts of the country, from upstate New York to South Dakota and dozens of other locations, that had seen little worksite enforcement activity in the past 20 years. The agency has similarly reached deeper into businesses that hire illegal aliens, prosecuting not only owners but managers, human resources personnel, a union steward and others who help illegal aliens get work; in one Missouri case, a federal grand jury indicted a receptionist. Much as prosecutors routinely seize the assets and profits from drug dealing, they have begun targeting assets and cash profits tied to the employment of illegal workers. In some instances, severe penalties have been imposed for employing a small number of people: One Ohio employer lost his home, valued at $770,000, for employing four aliens. Even individual workers are sometimes going to prison, in part because of the realization that even the simplest type of identity theft—using someone else's Social Security number to get a job—is not a victimless crime.

To accomplish such goals, ICE and prosecutors are dusting off long-unused laws to charge individuals with crimes associated with illegal employment. This shift in policy, with no change in the underlying laws, has been the most significant development in immigration enforcement since the passage of the Immigration Reform and Control Act of 1986 (IRCA), when employer sanctions and the I-9 form first came into effect.

ICE has also broadened its arsenal of investigative tactics. In Portland, Oregon, for example, ICE conducted an undercover operation to investigate allegations of criminal violations by employees of a national firm, American Staffing Resources, that recruits workers for a fruit and vegetable processing plant operated by Fresh Del Monte Produce. During that investigation, an informant engaged in

In the last two years the government's enforcement efforts have succeeded in driving home the point that employers ignore immigration law at their peril.

discussions with Del Monte personnel and managers of the staffing company about counterfeit documents and immigration issues. More than 100 temp agency workers were arrested. In Texas, undercover agents posed as workers at chicken processing facilities owned by Pilgrim's Pride Corporation, the nation's largest chicken producer, in an effort to infiltrate a reported network of illegal immigrants who were being required to pay hundreds of dollars to secure jobs. In fact, the use of undercover agents is now common.

But while employers have sometimes complained about being unfairly singled out for investigation, the ICE raids and other enforcement actions are anything but random. Indeed, they have tended to target employers who exploit illegal workers; who brazenly disregard the law; who do more than simply hire illegal aliens (for example, who help them come to the U.S. illegally); or who help criminals and fugitives.

Conclusion

These changes have not come without controversy. Some critics ask whether ICE and DHS have gone too far, threatening and sometimes imposing too-severe measures against employers who are vigilant and who follow required employment verification procedures. Others question whether the government gives employers sufficient tools to combat illegal employment and identity theft. The government's "E-Verify" program, for example, will confirm the employment eligibility of any employee whose name and Social Security number match those in the Social Security Administration database. But the system cannot distinguish between one situation where the right person has been hired and another that involves an impostor.

The questions go on and on, but in the short term they are not as important as the reality that business owners and managers must confront. With comprehensive immigration reform all but dead in Congress, 2008 likely promises more of the same, perhaps with some shifts in tactics. Some critics, for example, have called for ICE to focus more on the individuals and syndicates that traffic in fake documents and stolen identities; those who transport, house or otherwise aid illegal aliens; criminals and fugitives; aliens who steal citizens' or legal residents' identities; and employers who exploit workers. Regardless what the government ultimately decides is the fairest or most effective way to combat illegal immigration, the fact is that worksite enforcement is here to stay, in one form or another. New immigration legislation won't change that. Even the most amnesty-oriented immigration bills will require a foundation of strong enforcement if they are to have any hope of being signed by the next president, whether Democrat or Republican.

In the last two years the government's enforcement efforts have succeeded in driving home the point that employers ignore immigration law at their peril. For 2008, especially in highly targeted industries—construction, janitorial services, meatpacking, restaurants, agriculture and others—employers need to be proactive and make immigration compliance a high priority. Preferably before ICE arrives at the door. FB

The New EU Health Claims Regulation: Tightened Rules for Advertising and Labeling of Foodstuffs

By Christian Falk

An associate in Faegre & Benson's Frankfurt office, Christian Falk works in the firm's litigation practice. He can be reached via email at cfalk@faegre.com.

New rules regarding the nutrition and health claims made in the advertising, labeling and presentation of foodstuffs took effect in the European Union on July 1, 2007. Companies that produce and market foodstuffs in the EU need to understand the new rules, which are mandated by European Commission Regulation No. 1924/2006 of December 20, 2006, the so-called "Health Claims Regulation" (HCR). The HCR imposed new restrictions on the advertising and labeling of foodstuffs, which took effect immediately, and additional provisions of the legislation will gradually increase those restrictions in the next few years. As enforcement of the HCR and the new rules on nutrition and health claims gradually increases, a flood of lawsuits is expected, especially from consumer protection associations. This article provides an overview of the HCR and the new nutrition and health claims rules.

By enacting the HCR, European legislators have significantly tightened the legal framework for the advertising of foodstuffs throughout the European Union. In addition to the stricter substantive legal requirements concerning nutrition and health claims, the HCR also implements a systemic change: Nutrition and health claims are no longer solely subject to inspection after products reach the market. In the future, the only nutrition and health claims that will be allowed are those that are expressly permitted by the regulation. Statements relating to health will be subject to an official authorization procedure, which must be completed before a product may be sold. The European Food Safety Authority (EFSA) is responsible for evaluating health claims, including those related to the reduction of disease risk.

Current Effects

Standard Conditions for Acceptable Claims

The HCR's standard for acceptable nutrition and health claims introduced several new requirements. First, the HCR requires that any claims about the nutritional or physiological effects of a product be scientifically provable. Second, the new regulation requires that a substance with a claimed beneficial effect be found in the product in a form and quantity that are available to the human body—that is, the claimed beneficial effect must be realizable with the substance in the form and quantity found in the product. If a company is not able to prove those elements in a disputed case, then its advertising will be deemed illegal.

In many cases of claims related to nutrients, the proof of such beneficial effect will not be difficult (e.g., "rich in natural vitamin C," given that no vitamin additive was used and the product is in fact naturally rich in vitamin C). However, nutrition claims

that refer to a so-called "other substance" are subject to increased scrutiny under the HCR. The law defines "other substance" as "a substance other than a nutrient that has a nutritional or physiological effect."

Broadening of the Meaning of the Term "Nutrition Claim"

Under the HCR, the term "nutrition claim" is broadly defined; indeed, the regulation expressly applies to "other substances" in addition to nutrients. Until now, German and EU law concerning nutrition claims applied solely to substances with nutritional characteristics. In this respect, any food ingredient that is not a nutrient (e.g., enzymes) was not of concern. But the HCR defines a "nutrition claim" as any claim that "states, suggests or implies that a food has particular beneficial nutritional properties due to (a) the energy (calorific value)…and/or (b) the nutrients or other substances it (i) contains; (ii) contains in reduced or increased proportions; or (iii) does not contain."

The HCR does not define specifically what "other substance" includes, but a conservative reading of the regulation suggests that it would include plant and herbal extracts in the category of "nutritional claim." Thus, the mention of plant and herbal extracts on a product label, for example, could easily be understood as a nutrition claim, with the result that the selling company would have to prove scientifically the positive nutritional or physiological effect of an extract.

Special Conditions for Use of Certain Nutrition Claims

In addition to those general conditions, there are special conditions for nutrition claims under the HCR. Certain claims, such as "low fat," "rich in fiber," "rich in vitamin C" or "sugar free," can only be used for advertising and on labels if they fulfill the law's "conditions for use"—conditions that are defined in a list, which is attached as an annex to the HCR. The term "sugar free," for example, is only permitted if the product does not contain more than 0.5 grams of sugar per 100 grams or milliliters, while the claim "low sugar" may be used to promote a product if it does not contain more than five grams of sugar per 100 grams or milliliters. Nutrition claims other than those contained in the annex that were legally used in a member country before January 1, 2006, may be used until January 19, 2010. After this cutoff date, however, the conditions specified in the annex are definitive, and any claims that do not satisfy those conditions are forbidden.

Nutrition Labeling Also for Health Claims

The obligation to apply nutrition labeling rules in the case of the voluntary use of nutrition claims, which resulted some time ago from another EU directive, now extends, as a result of the HCR, to voluntary health claims. Based on the product's nutrition labeling, consumers should be able to determine the concentration of calories, fat, protein, carbohydrates and other nutrients, such as salt, sugar and saturated fatty acids. Additionally, the regulation requires that substances which are the subject of a nutrition or health claim, but that previously did not have to be included in nutrition labeling, must be listed, with their quantity, in the same field of vision in the direct vicinity of the nutrition labeling (e.g., peppermint extracts 0.1 g).

Future Effects

Nutrition Profiles

In addition to the new rules on nutrition and health claims that took effect on July 1, 2007, the HCR stipulates that the European Commission issue nutrition profiles. The profiles, to be issued by January 19, 2009, will specify threshold conditions of nutritional and health value and serve as a prerequisite to making any nutrition and health claims going forward. That is to say, certain foodstuffs and products in certain food categories will be required to meet the

conditions set out in the nutrition profiles in order to be able to display any nutrition or health claims at all. For example, if a food does not meet the requirements of a nutrition profile with respect to sugar, fat or salt content, then any nutrition or health claim advertisement and label information will be forbidden—without consideration of the truth of such information. This rule means that food must be conducive to healthy and balanced nutrition when viewed from its overall nutrition profile—in particular, with regard to fat, sugar and salt content—in order to be advertised with any nutrition or health claim at all. Thus, for example, it would not be permissible to advertise a product as "low fat" if it has a high sugar content that makes it not conducive to healthy and balanced nutrition.

Stricter Requirements for Health Claims

Under the HCR, health claims (for example, "strengthens your natural defenses" or "promotes bone formation") will be subject to stricter requirements in the future. The HCR divides such claims into three categories: (1) claims concerning the reduction of the risk of diseases; (2) claims about the development and health of children; and (3) other health claims, such as those that refer to the role of a nutrient or other substance. Interestingly, the health claims in the first category (i.e., risk reduction claims)—for example, "the regular consumption of sufficient amounts of calcium reduces the risk of contracting osteoporosis as you get older"—are not permitted currently under German law even if they are demonstrably true. However, they will be permitted under the new regime mandated by the HCR. Thus, while the general thrust of the HCR is to tighten restrictions governing health claims, in some cases, both in Germany and elsewhere, the HCR is actually more liberal than previously existing laws.

In this new regime, health claims in the third category will be permitted only if they are included in a list of generally permissible claims, which still must be prepared by the European Commission. The Commission's list will only contain claims that have a scientific basis, and claims included in the list may be used without approval. The HCR mandates that the list be published by the Commission and approved by European legislators no later than January 31, 2010. Health claims in the first and second categories are only permitted after completion of an official approval procedure through the European Commission, administered by the European Food Safety Authority. Health claims included in such lists then may be used, in conformity with the conditions applying to them, by any food business operator.

Transitional Provisions

The HCR contains various other transitional provisions intended to provide guidance to producers and dealers as they adjust to the new regulations. These provisions are too numerous and complicated to summarize here. Suffice it to say that producers and dealers will want to seek guidance from legal counsel as they work to comply with the HCR.

Summary and Outlook

Looking forward, the principle that "what is not expressly permitted is forbidden" will apply to nutrition and health claims in the advertising, labeling and presentation of foodstuffs in the EU. Some health claims will be subject to prior approval. Other nutrition and health claims will have to be grounded in scientific evaluation and be affirmatively published in lists approved by EU regulators. Given that these lists have yet to be written, that the HCR introduces a complicated regulatory regime, and that legal terms associated with nutrition and health claims are being redefined, there are tremendous uncertainties for producers and distributors of food products in the EU. Amidst so much uncertainty, it is clear that the EU Health Claims Regulation and the new rules it mandates will give competitors and consumer protection associations sufficient cause to go before the courts. FB

Last Word: Trusts and Estates

The changes put in place by the Economic Growth and Tax Relief Reconciliation Act of 2001 continue to be in force. Effective January 1, 2008, the gift and estate tax exemptions and rates are as follows:

- The federal estate tax exemption is $2 million.
- The generation skipping transfer tax exemption is $2 million.
- The top federal estate tax rate is 45%.
- The annual gift tax exclusion amount is $12,000.
- The lifetime gift tax exemption amount is $1 million.

States that have "decoupled" or separated from the federal tax system may have their own estate tax exemption amounts. As with the federal exemption amount, these numbers may change from year to year.

Although the federal tax exemptions did not change for 2008, changes will be on the way soon. The estate and generation skipping transfer tax exemptions are both scheduled to increase to $3.5 million on January 1, 2009. On January 1, 2010, the estate tax will be eliminated. On January 1, 2011, the estate tax will be reinstated to 2001 levels ($1 million exemption levels and a 55% top tax rate). As recently as 2005, permanent repeal of the estate tax seemed possible. However, momentum for repeal slowed during 2005 and with the election of Democratic majorities in the House and Senate in 2006, the chances of repeal appear slim. Given the unsettled nature of the law at this time, we recommend that you contact an attorney in our wealth management group to discuss your particular situation. FB

FAEGRE & BENSON LLP

2200 WELLS FARGO CENTER
90 SOUTH SEVENTH STREET
MINNEAPOLIS, MN 55402-3901

PRSRT STD
U.S. Postage
PAID
Minneapolis, MN
Permit No. 27100

The New Look of Immigration Enforcement
See Page 18