

## Inside

- 2...(R)evolution in the Law Firm Service Market
- 4...FTC Challenges Patent Holder's Refusal to Honor Predecessor's Commitment to License Patents Covering "Ethernet" Standard
- 5...Data Security Challenges for Retailers
- 7...Maintaining Credibility in FCPA Investigations

# FOCUS

## President's Message

**Mark Rogers**

To the chapter:

This spring has been a very successful season for the chapter! By the time you receive this edition of our quarterly newsletter, our (now) annual ethics series will have concluded—with chapter members earning collectively more than 175 hours of ethics instruction in time to meet annual CLE requirements.

As budgets tighten in tough markets, remember the chapter for your CLE needs. With programs chosen by us, tailored for in-house counsel, and costing you only \$15 per hour, the chapter is here to help you with affordable, high quality CLE.

We try to match up the substantive articles in the newsletter with the CLE programs, and we've been able to do that in this edition, with respect to recent and upcoming meetings. All three articles are from Perkins Coie, and we appreciate the firm's continued support of the chapter. There are some interesting recent developments in patent law, and one of the articles covers that field (you may recall a presentation by Perkins Coie on

patent law recently). Those of you who heard Al Gidari speak more recently understand at least some of the challenges surrounding data privacy and security, and there is an article that focuses on concerns of retailers in particular. The third article focuses on FCPA investigations, the subject of our June CLE.

Even as we complete the CLE year (for the Arizona calendar), we are busy making preparations for the programs later this year. Interest in sponsorships remains high, and we look forward to another full year of programs that will meet your needs and be of interest to you. Of course, if you have ideas for programs, please feel free to email them to [accarizona@yahoo.com](mailto:accarizona@yahoo.com) for consideration.

As always, (1) please help us increase membership when you hear of people moving in-house, (2) please consider attending the annual meeting (in Seattle this year), and (3) I hope to see you at an upcoming chapter meeting.

Mark Rogers

## Welcome

### New Members

We wish to welcome the following new members who have joined our chapter recently:

**Jacqueline Allen**, petSmart, Inc.

**Lorie Birk**, Mitel

**Lisanne Cottington**, Mitel

**Laura Eichelsderfer**, Apollo Group, Inc.

**Mark Fowler**, Barclay Group

**Mary Freeman**, Cytec Engineered Materials Inc.

**William Garr**, Contractor Management Services, LLC

**Karen La Madrid**, Western Adventist Foundation

**John Pons**, Cole Companies

# (R)evolution in the Law Firm Service Market

Susan Hackett

Senior Vice President and General Counsel, Association of Corporate Counsel (ACC)

Contact: [hackett@acc.com](mailto:hackett@acc.com)

**THESIS:** Traditional law firm business models for providing legal services and law school training for lawyers are not necessarily aligned with what corporate clients want: value-driven, high-quality legal services that deliver performance for a reasonable cost and develop lawyers as both savvy counselors and efficient business partners.

**THE PROBLEM:** Sometimes I feel like the “old lady of the in-house bar” (even at 47) ... I’ve been at ACC for close to 20 years. If one thing has remained a constant, it’s that members are less than satisfied with their outside counsel relationships. They may like their outside lawyers (or at least some of them), and they may agree that there’s incredible expertise out there—there is no shortage of smarts or talent. They may even tell you about the 4,017 different metrics and mechanisms that they employ to assure themselves that they’ve got a handle on their outside spend. But still ...

... Even in the best relationships, in-house counsel often don’t feel their outside costs are predictable or value-driven. Somehow or another, for all that they like in their outside lawyers, they have a lot of concerns regarding the firms they employ. Somehow or another, more time often is spent arguing over the bill after the fact than in setting expectations and goals upfront that everyone can manage to meet. Somehow, they feel that more precious time is spent on process than on counseling.

Another thing that hasn’t changed is that clients aren’t happy about their in-house lawyers’ inability to get a handle on their ever-increasing legal spend. The “inelasticity” of the price increases in the law firm business is, frankly, mind-boggling. In every other marketplace of services, prices go up and down with the economy or as new efficiencies or ideas surface and talent moves about. At firms, especially bigger firms, prices go up 6 percent per year, and we all have a sneaking suspicion that even if we negotiate a 10 percent price reduc-

tion on our matter, they’ll simply bill us for 15 percent more “service.” And all this happens at the same time that in-house departments, across the board, have decreased their own expenses, while at the same time increasing efficiencies and productivity.

Accordingly, a lot of very unhappy corporate counsel tell me that their corporate procurement departments are closely scrutinizing the legal department and their spend. And increasingly pressured managing in-house managers counsel look for the fix: they host beauty contests, develop convergence strategies, apply collars and cuffs and whatever’s new in fee management, they set up dashboards and compare costs by firm and regions and matter type and turnaround time, and they spend lots of time training their lawyers to engage in early case assessment. While some have some success (and while none of these are “bad” ideas), at best, all this tinkering does little more than rearrange the deck chairs on the Titanic.

Some blame the ubiquitous billable hour and its perverse drivers toward inefficient and terribly expensive results. Some blame the morph of law firms (professional entities) to a business model (profit driven). Others point to the almighty “profit per partner” ratings, highly leveraged pools of stunningly inexperienced and overpriced associates, and an increasingly de-equalized middle class of partners. Indeed, one of the most disturbing trends in all of this mess and despite the tall stacks of money paid out by clients is the incredible number of lawyers who are either pushed out of the profession, or run screaming from the building, often before they’ve enjoyed any semblance of the career and professional fulfillment we all envisioned we’d have when we were in law school.

In-house counsel from large departments, small departments, and every kind of company in every kind of industry are very powerful people and we can choose to hire

whom we want—everyone says so, right? And yet, we just can’t seem to get outside counsel and their costs “under control.”

**THE SOLUTION:** So I say: Time to roll our sleeves up and talk about what we *can* do if we work together to create long-term institutional change, rather than railing that everything we try on our own doesn’t return results consistent with our expectations—nothing changes on the larger scale.

**Revolution + Evolution = (R)evolution?**

**SETTING EXPECTATIONS:** I recognize that nothing anyone can do will change everything overnight, and lots of different folks want lots of different things, so there’s not even consensus around what success might look like even if we could envision it. So here’s what we ask and what we think is a reasonable expectation: join ACC in thinking like a revolutionary change agent (that is, thinking big picture and out of the box), but also help us implement real reform by working on evolutionary advances over time (that is, focus on practical solutions).

**The Proposition: ACC’s Value Challenge—Re-connecting value to the cost of legal services.**

**What ACC’s Value Challenge is and isn’t:** The value challenge is not an answer, but a movement. It’s not about laying blame; it’s about creating responsibility for change.

So let’s all agree that firms need to be responsible for addressing client dissatisfaction. And let’s recognize that no one’s saying that firms shouldn’t profit; on the contrary, firms must be sustainable entities. Let’s also get it straight: a focus on connecting cost to value does not mean that everything should be cheap or that we’ll lose our commitment to quality. There are lots of expensive lawyers out there who are worth every penny (the problem is the expensive lawyers who aren’t), and there are many high quality

lawyers who don't cost what some of their peers in big firm practices charge for the same services.

On the corporate counsel side, if firms are providing services we aren't happy with, why do we keep buying those services, thereby enabling inefficiency, inflated cost structures and poor practices? It's in-house counsel's responsibility to better manage their spend, help firms understand what we and our clients want, and reward outside counsel who deliver the outcomes we've asked for. If we're to convince corporate management that we know what we're doing, we better start recognizing that in 2008, no one gets hired or promoted just for retaining the expensive firms with big reputations. Regardless of their ranking status, in-house counsel will be evaluated for managing firms that provide value and results.

Accordingly, ACC will:

- promote intelligent and facilitated dialogue among corporate counsel, law firms, and eventually other stakeholders, including law schools, to help drive alignment and focus on value;
- develop methodologies and metrics that corporate counsel can use to assess the strengths and weaknesses of law firm vendors;
- create tools that in-house counsel and firms can share to drive change in the performance of valued legal services; and
- enhance awareness and promote communication of success stories in achieving value and alignment—creating practical benchmarking.

To accomplish these goals we're prepared to really dig in, dig deep, and commit ACC resources and stake our reputation for delivering results. While we have lots of ideas on tap and will be working on several plans concurrently, I wanted to use this forum to discuss an early role for chapter leaders and members:

**WHAT CAN YOU DO?—Getting Started.** We hope to engage members, local law firm leadership, ACC chapters, local and national bar groups, law schools, and other stakeholders to discuss what we should

do and how we should do it in a highly interactive discussion format involving small groups focused on delivering recommendations and direction. These conversations will cover a variety of topics, discuss best practices at work, help define "value" in legal services, discuss alternative models for law firms to use to conduct their business and to cost/bill their work, and really drill in on retention, training/development, and promotion of talent (at the entry level, in the middle ranks, and at the highest end of business). We will use the resulting intelligence to help shape more and better tools, resources, models for consideration, best practices and so on. In other words, we'll evolve together.

You will also be receiving an email soon (depending on publication dates, some of you may have already received it) from ACC's Value Challenge Steering Committee that asks you some simple survey questions that will allow us to collect some baseline information and feedback to target meaningful dialogue in these first sessions. Please watch for it and invest the 3-5 minutes it will take to complete this survey (it's online, so it's simple to do).

### **WHAT WE HOPE TO ACCOMPLISH: Desired Outcomes**

1. Create a national dialog about the need to reconnect value to costs, especially within the law firm community, with a common language and framework that ACC will have helped define and that our members will help drive.
2. Identify and empower core groups of leaders in the in-house and outside firm communities, as well as in consulting houses, vendor organizations, legal and business media, and the law school community: engage them and then solicit more participants every year.
3. Offer a tool kit for use by in-house counsel and another for outside firms (and shared resources, as well, of course), containing leading practices, management tools, models for managing value, and networks by which participants in this process can communicate their experiences and ask questions of each other, including "who do you use and how do you do this?"

4. Nourish the development of an in-house client community that gives law firms reasonable comfort that their efforts to implement change will be supported and rewarded.
5. Encourage law firms that are more focused on retention of talent valued by clients, and matter management driven by the client's expectations and needs.
6. Foster greater satisfaction and pride in their work for both inside and outside lawyers—spending less time bickering over bills and more time focused on solving client problems.
7. Ensure recognition by senior (non-legal) management that in-house counsel are taking the lead, rather than simply being reactive, and that they are exercising strong business skills in balancing their inside and outside legal spend—targeting results and outcomes, rather than just hoping to manage an unpredictable process.

*All of this is in pursuit of perhaps the most important outcome: a legal profession in which all attorneys deliver value.*

As the "increasingly mature" lady of the in-house bar, I see this initiative as the culmination of my career with this organization to date; yeah, I guess that makes it personal for me. But if these problems, and your dissatisfaction with the way things are is personal to you, too, please join me in starting the ACC Value Challenge (R)evolution. We here at ACC can think of nothing that's more *valuable* that we can offer you, your clients and our profession.

Susan Hackett: [hackett@acc.com](mailto:hackett@acc.com)

# FTC Challenges Patent Holder's Refusal to Honor Predecessor's Commitment to License Patents Covering "Ethernet" Standard

The Federal Trade Commission recently announced a complaint and settlement with Negotiated Data Solutions LLC (N-Data) alleging that N-Data engaged in unfair methods of competition and unfair acts or practices in its enforcement of patents against makers of computer equipment employing Ethernet, the dominant computer networking standard. The complaint was controversial because the agency challenged N-Data's conduct under the Federal Trade Commission (FTC) Act alone—it did not include parallel allegations under the Sherman Act. The agency also used theories that are generally pursued in FTC cases involving deception of consumers, rather than sophisticated business customers like computer makers.

## Background

NWay technology enables devices at opposite ends of a local area network to exchange information and automatically configure themselves (called "autonegotiation") to optimize communication. In 1994, National Semiconductor Corporation (National) held patents governing NWay technology. National agreed with the Institute of Electrical and Electronics Engineers (IEEE) that if the institute adopted a standard based on National's patented NWay technology, National would offer to license the technology for a one-time, paid-up royalty of \$1,000 per license to makers and sellers of computers using the technology. IEEE agreed and adopted the standard.

N-Data licenses patents that it acquires from inventors or other patent holders. In 2003, N-Data acquired National's NWay patents. N-Data then began demanding that computer makers pay royalties on a per-unit basis for equipment sold incorporating NWay technology. The royalties were based on "reasonable terms and conditions" and equaled amounts far higher than the \$1,000 one-time royalty that National had agreed to charge. N-Data threatened or sued firms that refused to pay the new per-unit royalties.

## FTC Enforcement Action

The enforcement action was controversial within the agency itself; the complaint was approved by only three of the five commissioners. The two dissenting commissioners made several key points:

First, unlike earlier cases challenging "patent holdups" in the context of standard setting, the original patent holder (National) had not been guilty of "bait and switch" tactics in 1994 when it offered to license its NWay technology on a flat, one-time royalty basis. Its offer was genuine.

Second, the facts were unclear whether the industry had actually taken up National on its offer. Many manufacturers simply used National's technology without paying the \$1,000 license fee. That made it difficult to characterize N-Data as having breached a contractual obligation to industry members.

Third, to the extent N-Data's conduct victimized anyone, the victims were sophisticated computer makers, rather than individual consumers and small businesses. By invoking the FTC's consumer protection authority on behalf of sophisticated business consumers, the majority had improperly expanded the scope of that authority to matters traditionally analyzed under competition-related antitrust principles.

Finally, in voting on the complaint, the majority had noted that, because the consent decree did not include alleged violations of the Sherman Act, it would not lead to follow-on litigation by private parties seeking treble damages (FTC Act § 5 does not provide a private [right?] of action). The dissenters noted, however, that the majority had ignored that many state antitrust statutes were modeled after FTC § 5 and do provide private rights of action. So follow-on litigation is possible, if not likely.

## Recommendations

In light of the consent decree, firms engaged in standard setting should:

1. Limit their participation in standard-setting programs to technologies central to their businesses;
2. Be explicit about any contractual obligations they incur regarding technology licensed to comply with a standard;
3. If buying or licensing technology from another firm, investigate fully any commitments—formal or informal—that firm may have made in the course of standard-setting programs; and
4. Be aware—not only of the potential for private actions under state FTC Acts for "unfair" conduct similar to that of N-Data, but also of the risk of being subjected to a potentially lengthy administrative proceeding within the FTC before an administrative law judge (ALJ) where federal court review is not available until after the ALJ has overseen full-blown discovery and conducted an administrative trial and the full commission has issued an opinion on the appeal of the ALJ's decision.

*A Perkins Coie Update reprinted with permission by Perkins Coie LLP and Affiliates*

# Data Security Challenges for Retailers

As the news is increasingly filled with reports of identity theft and the data security breaches experienced by large retailers such as TJX, several groups are expressing concerns about the safety of sensitive consumer data. Although, as discussed below, there is an existing standard for safeguarding this data, compliance with that standard is far from universal. Additionally, many of the mandates faced by merchants are inconsistent and sometimes in conflict with each other. With the cost of data security breaches rising and public awareness and anxiety increasing by the day, retailers need to be more aware than ever of how to keep customer data out of the wrong hands. Below we have outlined some recent developments in the area of payments and data security breaches and offered some suggestions for keeping data secure.

## Current Data Security Landscape Retailer

### Compliance With the Existing Data Security Framework Is Inconsistent

The Payment Card Industry Data Security Standards (commonly referred to as “PCI,” “PCI-DSS” or the “PCI Standards”) were developed by the credit card associations to require merchants and card transaction processors to maintain a high level of security around cardholder data. The standard requires, among other things, that retailers build and maintain a secured network, firewall cardholder data from the rest of its network and encrypt transmitted cardholder data. Although the deadline for merchant compliance with PCI has passed and the card associations have boosted their collective efforts to force compliance by issuing fines for noncompliance, Visa recently estimated that only 77 percent of the largest retailers and 66 percent of mid-sized retailers are currently certified as compliant with PCI. That figure means that about 75 of the nation’s largest retailers are not yet PCI-compliant. Although the cost of PCI compliance is high, failure to comply can result not only in fines, but in increased transaction fees imposed by the card associations. This past summer, Visa issued \$880,000 in fines to Fifth

Third Bank for the TJX breach. Additionally, if improper data security leads to a data breach, a merchant bank may be liable for the cost of reissuing cards and reimbursing customers for fraudulent transactions, as well as the attendant costs of handling customer claims and notifying customers of a breach. The merchant banks typically have strong contractual indemnification rights against merchants for such losses. TJX recently settled with Visa-issuing banks for \$40.9 million and estimated that its pre-tax charges for the data breach would be approximately \$216 million, which makes it clear that the cost of handling (or mishandling) sensitive data can quickly become unsustainable for even large retailers.

### To Store or Not to Store, That Is the Question

Retailers are wrestling with the conflicting card association requirements that they (a) not store cardholder or transaction data beyond the time it takes to process a transaction and (b) be able to later retrieve certain pieces of that same information to facilitate investigation of chargebacks and other issues. Although the card association rules expressly prohibit merchants from retaining or storing PINs, magnetic stripe information and other sensitive information subsequent to the approval of a transaction, the same rules impose on merchants an obligation to provide copies of the transaction receipts, including account numbers, cardholder names and card expiration dates, to issuing banks trying to investigate cardholder chargebacks and claims of error or fraud. The association rules mandate strong security measures for all material containing account numbers, such as transaction receipts, but they do not permit a merchant to decline to keep such material in the first place.

### Retailers Are Demanding Change

The National Retail Federation (“NRF”), the world’s largest retail trade association, offers an alternative solution to what it deems the unfair and risky data security requirements imposed by the card associations. In a letter dated October 2, 2007 to Bob Russo, general manager of the

PCI Security Standards Council, David Hogan of the NRF explains that the goal of safeguarding customer transaction information would be better served by simply reducing the amount of information merchants are required to retain rather than forcing merchants to comply with the burdensome PCI standards. Hogan claims that it would be easier for the card associations (i.e., Visa and MasterCard) to protect the transaction data “from thieves by keeping it in a relatively few secure locations than to expect millions of merchants scattered across the nation to lock up their data for them.” “Much has been said about PCI being a moving target, and how retailers have been forced to jump through extraordinary hoops in the quest to achieve compliance . . . but a primary reason that PCI exists . . . is because credit card company rules require merchants to store the credit card data that criminals are so eager to steal.” Hogan makes an interesting point. Arguably, merchants across the country are scrambling to comply with the PCI standards when an easier solution might just lie in centralizing the information retention responsibilities. He suggests that merchants should be required to retain only the authorization code proving the transaction was authorized and a truncated version of a receipt. These two things, he argues, should provide verification that the transaction has been approved and allow enough information for a customer return, but not provide a full account number or anything of value to a potential thief. Although his suggestion may not be the ultimate answer, it certainly evokes thought and illustrates how some creative problem solving on the part of other participants in the industry may result in more effective and efficient solutions than continuing to rely on instructions from the card associations.

### States Are Giving PCI Standards the Force of Law

The NRF letter comes on the heels of the attempts by several state legislatures to codify the core PCI requirements. Although many states already have laws that address responsibility for notifying customers in cases of data security breach, in May 2007, Minnesota became the first

state to enact a law that places liability for data security breaches squarely on merchants that are found to have stored transaction data in violation of the PCI standards.

Several other states are in various stages of considering similar legislation, but no similar bills have been enacted as of yet. Without such laws, liability for data security breaches will be allocated by the rules of the card associations and the contracts between merchants and their banks. Under the card association rules, the merchant bank is typically liable for any damages resulting from improper data storage procedures by its merchant and it has to seek indemnification from the violating merchant for any resulting damages. Such damages, which, as discussed above, can include the cost of customer notification, reissuance of cards, credit monitoring for the effect on cardholders and reputational damage to the issuing bank, were recently estimated by Forrester Research to be between \$90 and \$305 - with the top end involving high-profile breaches in highly regulated industries such as banking.

### Federal Enforcement Efforts

In addition to fines and expense reimbursements imposed by the card associations and state legislatures, violations of data security and failing to adequately implement a privacy policy can result in unwanted attention from the Federal Trade Commission for engaging in deceptive practices. Online retailer “Life is Good” recently settled an enforcement action brought by the FTC that charged Life is Good with making deceptive security claims and violating federal law. Apparently, although the retailer’s privacy policy purported to maintain all sensitive information in a secure manner, the reality was that Life is Good, among other things, “unnecessarily risked credit card information by storing it indefinitely in clear, readable text on its network, and by storing credit security card codes; [and] failed to assess adequately the vulnerability of its website and corporate computer network to commonly known and reasonably foreseeable attacks, such as SQL injection attacks.” The FTC also found that Life is Good failed to “implement simple, free

or low-cost, and readily available security defenses to SQL and similar attacks; failed to use readily available security measures to monitor and control connections from the network to the Internet; and failed to employ reasonable measures to detect unauthorized access to credit card information.” The FTC alleges that as a result of Life is Good’s general failure to adequately protect sensitive information, a hacker employing a SQL injection attack was able to obtain the credit card information of thousands of customers. The settlement requires that Life is Good employ several measures to ensure that it adequately protects information it receives and that its privacy policy appropriately reflects the company’s actual information-handling practices. This settlement underscores the importance not only of employing adequate data security measures, but also of providing an accurate privacy policy to consumers.

### Alternative Approaches

#### New Software Standards

In addition to the PCI standards, some alternative measures to protect sensitive data are already in the works. The PCI Security Standards Council is drafting a set of standards for the makers of payment-processing software that would prohibit such software from storing certain information. The draft rules are called the Payment Application Data Security Standard (“PA-DSS”). The PA-DSS is based on Visa’s “Payment Application Best Practices” and would require that any software handling credit or debit card data not store or cache prohibited data from a transaction, including the information saved to a card’s magnetic stripe, the CVV2 (card verification value) security number or PIN (personal identification number). “Back in the day when anyone wrote an application, the thought was that always more data is better,” said PCI Security Standards Council’s Russo. “In a lot of cases, the merchant doesn’t even know they are storing the data.” The fact that older software may be in use by some merchants has not been lost on the information thieves, however. Avivah Litan, a data security analyst at Gartner, believes that software applications that save prohibited data are likely already

being targeted by attackers. “Attackers like to find vendors whose products store data, and then find businesses that use those vendors,” she said. The proposed rules are now in a comment period, but will likely be adopted early this year. Even so, Russo estimates that given how expensive conversion will be, it will likely take two to three years before most retail systems are converted to the new software standard. The actual compliance deadline for PA-DSS is July 1, 2010.

### New Payment Methods

In response to heightened awareness of data security and the consequences of data compromise, retailers are increasingly looking to other vehicles that offer less risky methods of getting paid. In addition to PayPal, a relative “old-timer” in the alternative payments space, the recently launched Revolution Money is one such vehicle. On top of the promise of lower interchange fees to merchants, Revolution offers an anonymous card that bears only a magnetic stripe and a bar code, as well as transactions that are transmitted on a proprietary network. This solely PIN-based card can be used for credit or debit transactions both online and in brick-and-mortar locations. Merchants may prefer such an approach because a proprietary system eliminates legacy data storage issues that are common with the Visa or MasterCard systems. Also, cards without a name or account number on them will make it impossible for thieves to make purchases without the PIN or obtain any personally identifiable data about the cardholder. Many card issuers are also offering cardholders the option of obtaining single-use PINs for one-time purchases and other instances where security is a concern. Revolution is just one of several new entries into the payments space that is addressing data security issues as a core feature of a product.

### Recommendations

Although there are several developments in the payments space that may make data security less burdensome in the near future, merchants must continue to be vigilant to stay out of the headlines. Merchants may want to monitor devel-

opments such as the NRF letter or other efforts to effect change in the card association policies on merchant data storage responsibilities. Meanwhile, all merchants should review and implement the following recommendations from the FTC on appropriate information security policies and procedures:

1. Designate an employee or employees to coordinate the information security program;
2. Identify internal and external risks to the security and confidentiality of personal information and assess the safeguards already in place;
3. Design and implement safeguards to control the risks identified in the risk assessment and monitor their effectiveness;
4. Develop reasonable steps to select and oversee service providers that handle the personal information of customers; and
5. Evaluate and adjust its information security program to reflect the results of monitoring, any material changes to the company's operations or other circumstances that may impact the effectiveness of its security program.

In addition to the general measures listed above, all merchants should continually audit their existing payment systems and consider accepting less risky methods of payment. Below are some specific suggestions for ensuring that your information-handling procedures and software will keep your data safe:

1. Make sure your software does not store the contents of a payment card's magnetic stripe or the CVV, CVV2 or PIN. Review all current software to ensure it is not storing prohibited information.
2. Destroy stored information in a secure manner when it is no longer needed.
3. Develop and implement adequate firewalls.
4. Comply with security audits according to the PCI requirements. For details, see [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).
5. Do not use default passwords and security codes supplied by the software manufacturer to secure the processor's data and computer network. Passwords and security codes must be unique to your business.
6. Encrypt all payment card information stored on the processor's computers.

7. Encrypt any card data transmitted over the Internet or other open public network.

8. Use anti-virus software and keep it updated.

9. Keep other software, such as operating systems, secure and updated.

10. Provide employee access to data on a need-to-know basis only.

11. Give each company employee who uses a computer a unique ID.

12. Restrict physical access to hard-copy payment card data.

13. Test the company's security systems on a regular basis.

14. Have an information security policy that spells out rules for employees who handle data and reinforce it regularly.

*A Perkins Coie Update written by Veronica McGregor. McGregor is Of Counsel with Perkins Coie's Business Group and works in its San Francisco office.*

*Reprinted with permission by Perkins Coie LLP and Affiliates*

## Maintaining Credibility in FCPA Investigations

Federal enforcement of the Foreign Corrupt Practices Act (FCPA) is on the rise. As corporate executives and white collar practitioners well know, this federal statute — enforced by both the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) — prohibits payment of bribes by American companies to foreign governmental officials to advance a business interest. Stepped-up enforcement results from a combination of factors: an increasingly worldwide, global economy, a desire by the U.S. government to stem public corruption in this country and abroad, and a motivated and capable enforcement team at DOJ and the SEC. With this heightened focus on the FCPA, companies that have an international presence will at some point encounter an FCPA issue — it is inevitable. Companies

are best served when they recognize the government's enforcement priorities and respond to them in a strategic way unique to the FCPA.

While DOJ has made FCPA enforcement a priority and has pursued several significant cases — many of which have been prominently described on the front pages of newspapers across the country — it has done so with limited resources. At the DOJ Fraud Section, only a few prosecutors, currently supported by five FBI agents, are totally dedicated to FCPA enforcement. Other prosecutors from DOJ's Fraud Section and from U.S. Attorneys' offices assist on cases, but those lawyers work on a variety of matters and FCPA enforcement is not their full-time responsibility.

Because of the government's limited resources, it must triage the cases it sees and try to leverage its resources to accomplish as much as it can. This provides a terrific opportunity for a corporation to take control of its own destiny as FCPA issues arise. If the corporation can convince the DOJ that it is forthcoming, committed to full disclosure, and represented by experienced and trustworthy professionals, the government will often allow the corporation to conduct its own investigation, report the results of the investigation and implement self-defined remedial measures. For the company, this is far preferable to responding to grand jury subpoenas, FBI interviews of employees and all the other distractions and expenses associated with a criminal investigation. Certainly, it is far preferable to a criminal prosecution, the

likelihood of which is greatly reduced if the company can essentially fill the role traditionally filled by government investigators.

The key to being permitted to control the fate of the company is to establish and jealously guard the credibility of both the company's FCPA lawyers and the company itself. Very often in FCPA cases – more so than in other white collar cases – companies decide to voluntarily disclose allegations of wrongdoing. How disclosure is handled will often decide whether the government will devote some of its scarce resources to the matter, or will count instead on the company to provide the government with information.

Here are some tips:

1. The company should choose a lawyer who will have credibility with the government as being trustworthy and experienced in conducting FCPA investigations. The government wants to know it has a surrogate upon which it can rely. For example, the pedigree of a former federal prosecutor (i.e., former Assistant U.S. Attorney or DOJ Trial Attorney) usually provides comfort to the government sufficient to allow the internal investigation to proceed under the company's direction. Similarly, the experience of a lawyer who has investigated FCPA matters will reassure the government.
2. Assume at all times that the government is watching every step of the investigation. Maintaining such a mindset will keep the lawyer and company on track to react quickly, gather and preserve all relevant facts and take appropriate remedial measures. This is a wise approach, even if the company ultimately concludes that a voluntary disclosure is not appropriate.
3. Disclosure is about revealing the facts, not litigating the matter. An FCPA disclosure is different than the typical discussion with a prosecutor over whether a case should be pursued. It will not be helpful to the company in the long run to shade the facts, or to be overly selective about what facts are disclosed. If the government believes that it is not receiving all the relevant facts in a forthright manner, the lawyer and the company will have sacrificed their credibility and once sacrificed it can never be retrieved.
4. The objective of the disclosure is to convince the government that it need not devote resources to the case. To that end, all materials shared with the government should be well organized, clear and presented in a manner consistent with the seriousness of the allegation so the government does not need to spend time trying to figure out what it has been provided. Doing so shows the government that the lawyer and the company are interested in presenting the information to the government in an understandable way, as opposed to simply dropping a stack of paper at the government's feet.
5. The disclosure is not the time to argue the law. There will be plenty of time to talk about the consequences. Debating the law will send the signal to the government that the lawyer is advocating, not disclosing, and as a result the government will begin to question whether it is being provided the straight story.
6. Take care to establish that the company is responsible, understands its obligations to comply with the law and is committed to doing so. This is done by demonstrating that corporate ethics guide the very top of the company, and are disseminated throughout the company by training, awards, messages and other avenues. Think carefully about whether to bring a client representative to the disclosure meeting who can help establish this point, but avoid bringing a client representative who is a fact witness.

7. Understand that the government will use a voluntary disclosure, even one that results in no action, as an opportunity to “kick the tires and look under the hood” of a company's policies. The company should not resist those efforts or be defensive about them. Demonstrating a legitimate interest in having an effective and robust compliance program is essential to resolving an FCPA allegation on favorable terms.

Of course, voluntary disclosure is not the right course in all FCPA matters. Many factors may affect this call, including the seriousness of the conduct, the country at issue, and whether the matter must otherwise be disclosed in public SEC filings. But in the many cases where disclosure is appropriate, the manner of the disclosure is critical. If confrontational and difficult, the disclosure can lead to a heightened government involvement and distrust. But if handled with a cooperative approach, the disclosure can foster respect and trust by the government, and often a less severe result. Taking a few small but meaningful steps to establish and maintain credibility will pay enormous benefits for the company and the lawyer in the long run.

*Written by Lee Stein, a litigation partner at Perkins Coie Brown & Bain P.A. Stein is co-chair of Perkin Coie's Investigations and White Collar Defense Practice Group. Reprinted from Criminal Justice Section Newsletter, published by the American Bar Association Criminal Justice Section.*

## Board Members and Contacts

### President

#### Mark Rogers

Vice President, Corporate Counsel & Assistant Secretary  
Insight Enterprises, Inc.  
480.333.3475  
mnrogers@insight.com

### Secretary

#### Gary Smith

Attorney  
602.284.7491  
audric@cox.net

### Treasurer

#### James Curtin

Managing Corporate Counsel  
Allied Waste Industries, Inc.  
480.627.2381  
jcurtin\_phx@msn.com

### Board of Directors

#### Kelleen Brennan

#### Catherine Brixen

#### Margaret Gibbons

#### David Glynn

#### Kevin Groman

#### Ruth Hay

#### Robert Itkin

#### John Kaminsky

#### Virginia Llewellyn

#### Mary Beth Orson

#### Steven Twist

#### Cyndy Valdez

#### Paul Ward

### Chapter Administrator

#### Karen Rogers

accarizona@yahoo.com

## ACC News

### ACC Seeking Nominations for “Excellence in Corporate Practice”

ACC is now accepting nominations for the 2008 “Excellence in Corporate Practice” award for exemplary achievement within the in-house legal profession. Nominees must have achieved success in one or more areas involving services and contributions to the legal profession. Nomination forms must be received no later than July 1, and awards will be presented October 19–22 at ACC’s 2008 Annual Meeting in Seattle, WA. For the 2008 nomination form and a list of past recipients, visit [www.acc.com/php/cms/index.php?id=282](http://www.acc.com/php/cms/index.php?id=282). For information on the Annual Meeting, visit [am.acc.com](http://am.acc.com).

### Recruit a Member and Win A Prize—Guaranteed!

Each time you use the Association of Corporate Counsel network, you gain valuable skills and experience only available through ACC. More members in ACC translate into improved educational opportunities, enhanced networking, increased online resources, and advancement of the profession worldwide. You can help expand your ACC network by taking part in the “Everybody Wins” membership drive. When you recruit new members to ACC, you will win prizes ranging from complimentary \$5.00 Starbucks’ cards and cutting edge electronics including portable DVD players, digital cameras and new computers, to free ACC Annual Meeting or ACC Europe Annual Conference registration and a \$750 travel stipend. ACC’s “Everybody Wins” membership drive ends on August 30—so don’t delay, recruit today! Learn more at [www.acc.com/everybodywins.com](http://www.acc.com/everybodywins.com).

### Get Access to Timely Hands-On Advice with ACC Top Ten

The ACC Top Ten provides summaries and hands-on advice regarding current legal issues affecting in-house practitioners. View a recent top ten on things to remember when preparing executives for deposition testimony at [video.acc.com/toptenfeb08.cfm](http://video.acc.com/toptenfeb08.cfm). A first for ACC, this Top Ten features video vignettes of “what not to do” while being deposed.

### It’s Never Too Early to Register for ACC’s 2008 Annual Meeting

Spring may be nearing an end, but don’t let summer pass you by without registering for the educational and networking event of the year for corporate practitioners. ACC’s 2008 Annual Meeting (October 19–22, Washington State Convention & Trade Center, Seattle, WA) includes over 100 CLE sessions providing practical advice on a broad range of legal specialties, with special sessions for new in-house counsel, new legal managers, chief legal officers, small law department practitioners, and much more. You cannot afford to miss this meeting. October will be here before you know it so make sure to register now at [am.acc.com](http://am.acc.com). Questions? Contact ACC’s education department at [education@acc.com](mailto:education@acc.com).

### Tap into ACC’s Global Network through MemberToMember<sup>SM</sup>

You’re invited to join the nearly 2,000 ACC members who have volunteered to share their knowledge on more than 100 substantive law issues with other members in ACC’s MemberToMember<sup>SM</sup> network ([www.acc.com/member-2member](http://www.acc.com/member-2member)). This unique online peer-to-peer community links you to other members seeking guidance by learning best practices from real-world applications. Participate as a volunteer expert or use this network the next time you run into an issue where advice from another in-house attorney might prove to be beneficial. Tap into ACC’s global network today for practical solutions and ideas to better serve your company. Questions and/or recommendations can be sent to [membership@acc.com](mailto:membership@acc.com).