TOPICS COVERED // *Risk & Trends*

# CARTEL ENFORCEMENT

## How Well Do You Know the Risks of Information Exchange?

Written by Paul Friedman, Rony Gerrits, and Michael Kniffen

In the popular imagination, cartels are associated with hardcore criminal activity. Cartels evoke images of smoke-filled backrooms where shady characters cut deals to line their own pockets, or perhaps media reports of gangs who distribute drugs. Rarely is the word associated with business-minded employees who bump into their counterparts at suppliers' meetings or trade associations, or merely meet to discuss industry issues of mutual interest.

Yet these informal exchanges—sometimes planned and sometimes by happenstance—can push companies into the crosshairs of cartel enforcement agencies in Europe and elsewhere.

Cartel work is big business for global enforcement agencies. In Europe alone, the European Commission (EC) has raked in over €19.7 billion in cartel fines since 2000. These fines have hit corporations across industries—from automotive-parts suppliers and LCD manufacturers to airfreight carriers and banking institutions. Understanding the risks faced by your company is vital in today's agressive enforcement climate. It is all too common—and potentially costly—to ignore cartel enforcement trends and the risks of information exchange.

**What Is Cartel Enforcement?**

In most jurisdictions, cartel enforcement involves investigating agreements among competitors designed to suppress competition. An agreement to charge an inflated price for a product or service is one example of a cartel agreement, but the agreement doesn't have to be about price. Competing companies might agree on production quotas, for example, calculated to limit supply and thereby indirectly boost prices. Even if employees don't always associate this behavior with the popular idea of "cartels," they generally understand that agreements with competitors to fix prices or manipulate supply are illegal.

Employees get into trouble, however, when they operate as if something short of an "agreement" is safe. This typically occurs when employees are tasked with gathering market intelligence and decide that exchanging information with competitors provides a useful data point that the company can consider along with other sources of information. Even when employees recognize that there is some risk in talking with competitors, they too often minimize the dangers of these exchanges by persuading themselves that they didn't reach "agreements" with competitors. For instance:

- Some employees explain that they don't know if a competitor is telling the truth—which they take as a prerequisite for an agreement.
- Others say that they don't know exactly what a competitor will do. To them, this uncertainty means that there is no "agreement."
- Some feel protected because an agreement to them means a formal, written document.
- Others understand that formal agreements (or even informal handshakes) are unnecessary to seal the deal, but nevertheless feel protected because they've been taught that information exchange alone is insufficient to trigger legal liability.

None of these explanations are persuasive to the EC and some other enforcement agencies, and they are often regarded as irrelevant as a matter of law. In fact, surprisingly few employees understand that exchanging information is itself a serious compliance issue because it can be used as evidence of an underlying agreement. Fewer still appreciate that information exchange alone can trigger liability in some jurisdictions such as Europe.

**The Risks of Information Exchange**

Information exchange refers to sharing commercially sensitive information. In the United States, information exchange can be used as evidence to infer an illegal agreement. The idea is that competitors would not share sensitive commercial information absent some agreement or understanding that the information would not be used against them. While US enforcement agencies target "agreements" (although the Federal Trade Commission has reached consent decrees in civil actions based on pure information exchange), there is no need to prove an underlying agreement in Europe. Instead, the law prohibits "concerted practices"—a concept that is broader and more flexible than an "agreement."

**Figure 1**

Information exchange includes, among other things, sharing information about past, current, or future:

- Prices
- Production quantities
- Production costs
- Turnover
- Sales
- Capacity
- Customer lists
- Marketing plans

A "concerted practice" is a form of practical cooperation between companies that is knowingly substituted for the risks of competition. Exchanging information at suppliers' meetings, trade association meetings, or by telephone or email all qualify as concerted practices. In principle, the law also requires some evidence of implementation, but it presumes that a company takes into account information learned from a competitor when determining its own conduct in the market. The upshot is that merely exchanging commercially sensitive information with competitors is an actionable violation in Europe.

Sensibly enough, the EC is unlikely to target an isolated incident of information exchange unless the Commission sees a pattern of similar behavior. However, your company does not have to participate in all information exchanges—or even a majority of them—for liability to attach. Similarly, there is no need for every competitor to share commercially sensitive information. As long as one company shares sensitive information, it is presumed that others at the meeting (or in the flow of information exchange) are part of that exchange. In fact, the only defense in Europe in these types of situations is when a company's representative publicly distances himself or herself (and, by extension, the company) from the discussion at the meeting. Silent disagreement is not enough.

In addition to pursuing information exchange as a "standalone infringement," the EC can also use information exchange to link companies to a "single continuous infringement" occurring over a longer period of time. The longer duration leads to increased exposure and potential fines.

**Strategies to Mitigate Risk**

Today, companies have increased opportunities to informally connect with competitors. In the tech industry, for example, companies often have "customer/supplier" relationships with companies in one area of the business and "competitor" relationships with those same companies in another. It is also common for companies to collaborate on research and development, and customer-mandated procurement processes often require supplier-competitors to exchange information. Add this to the list of trade associations, customer-sponsored suppliers' meetings, and regulatory associations, and you end up with a substantial list of touchpoints that all provide opportunities for offline discussions that increase compliance risks.

Understanding the dangers of information exchange is the first step in managing the risks of cartel enforcement. Beyond that, companies should consider other strategies to mitigate risk.

***Survey Your Company's Risks.***
Understand where your company faces compliance risks.

- Do you know how many trade associations you belong to? Are they all necessary?
- Do you have a list of customers that also compete with you in other areas?
- Do you know where your employees typically come into contact with competitors?

***Establish Clear Guidelines.***
Ensure that employees know how to interact with competitors.

- Establish fundamental rules.
- Create "do's and don'ts" lists.
- Provide regular training that focuses specifically on the hazards of information exchange.
- Train your employees on how to respond if someone shares sensitive information at an industry event.

***Create Structural Safeguards.***
Establish ethical walls between sales departments and planning/development departments.

- Ensure that employees don't wear multiple hats.
- Work from written agendas.
- Conduct internal audits.

### Author Biographies

***Paul Friedman*** *is a Partner in the London and San Francisco offices of Morrison & Foerster and heads the firm's global compliance practice. He specializes in conducting internal investigations on behalf of companies and audit committees, many of which are global in scope and focus on corruption issues, alleged price-fixing by cartels, and other compliance issues.*

***Rony P Gerrits*** *is Co-Chair of Morrison & Foerster's global Antitrust Law Practice Group and Managing Partner of the firm's Brussels office. He handles a wide range of competition matters, with a particular focus on global cartel cases. He has represented clients involved in cartel investigations in several industries, including cathode ray tubes, rechargeable batteries, smart card chips, auto parts, LCDs, freight forwarding, and optical disk drives, among others.*

***Michael P Kniffen*** *is a member of the Litigation Department in Morrison & Foerster's San Francisco office. His practice includes representing clients in criminal and administrative investigations brought by the Department of Justice, the SEC, and other global enforcement agencies.*