27 October 2021

Dawn raids are back on the agenda for competition authorities – is your company prepared?

Dawn raids are firmly back on the competition authorities' agenda. Recent European Commission (the "**Commission**") dawn raids in the animal health and wood pulp sectors signal the start of a new wave of unannounced inspections across Europe over the coming months, which will concern many different sectors and different types of suspected competition law violations. Now is therefore the right time to review and update companies' internal dawn raid response strategies, to ensure that they are effective and adapted to "modern" dawn raids.

Earlier this week, the Commission **announced** that it was conducting unannounced inspections (so-called "**dawn raids**") at the Belgian premises of a company active in the animal health sector, citing concerns that the inspected company may have infringed Article 102 TFEU (the EU antitrust rules prohibiting abuse of a dominant position). This follows hot on the heels of the Commission's **announcement** (on 12 October 2021) that it was conducting cross-border dawn raids in the wood pulp sector – on that occasion, citing suspected violations of Article 101 TFEU (the EU antitrust rules prohibiting cartels and other restrictive business practices).

These two inspections will not remain isolated incidents, and recent public statements by Commissioner Vestager clearly show a resurgent appetite for future raids. Indeed, it was only last week that Commissioner Vestager **suggested** that the raids in the wood pulp sector were "*just the start of a series of raids that we're planning for the months to come*", whilst also noting that the Commission's "*work on collecting evidence [would be] gathering pace*" (as already proven by the subsequent raids in the animal health sector). This resumption of activity had already been signalled in earlier comments made in June 2021 by the head of the Commission's cartel directorate, who noted that, although cross-border dawn raids had been "*very difficult and complicated to organise in the past 15 months*", the Commission was starting to tackle this backlog – with more raids planned for the autumn.

Numerous national competition authorities in the EU have also recently recommenced dawn raids with renewed vigour (or have at least signalled their intention to do so) – perhaps most notably in Greece, where the Hellenic Competition Commission has over the summer months conducted a significant number of different raids (across multiple sectors).

Clearly, the period of relative peace and quiet – a result of the COVID-19 pandemic, which forced competition authorities to suspend most inspections – is coming to an end. The recent dawn raids by the Commission are therefore best understood as the start of a new wave of raids across Europe over the coming months, concerning many different sectors and different types of suspected competition law violations.

Given these developments, companies should recognise that now is an ideal time to ensure that they have implemented a robust and up-to-date internal dawn raid response strategy. Importantly, any internal dawn raid response strategy must reflect the fact that the way in which competition authorities conduct dawn raids has evolved considerably in recent years (and that novel issues may therefore arise during a "modern" raid).

Our dawn raid guidance below provides a helpful summary of issues that a company should consider when updating its internal dawn raid response strategy, as well as a list of key "DOs" and "DON'Ts" that should guide a company during an inspection.

vbb@vbb.com
www.vbb.com

ARE YOU "DAWN RAID READY"?

The emergence of the "modern" dawn raid

Dawn raids are unannounced inspections of business/domestic premises, conducted by competition authorities to investigate suspected competition law infringements. Dawn raids enable authorities to search business premises, seize a wide range of hard-copy and/or electronic evidence and/or interview relevant employees. Such activities have for decades been a valuable tool for detecting anticompetitive conduct and supporting effective competition law enforcement.

Companies should recognise that the way in which competition authorities conduct dawn raids has evolved considerably in recent years. Largely gone are the days where sizeable teams of inspectors would descend upon multiple office locations and painstakingly sift through reams of (mostly hard-copy) documents over a number of days; rather, and given the far greater emphasis on electronic files and data, companies should now expect a much leaner on-site authority presence (perhaps even just a single official, together with an IT specialist) for a shorter period.

The ongoing COVID-19 pandemic will also present new challenges in this regard, in particular because a greater number of employees are now expected to be working from home more frequently. New issues that are likely to arise include: (i) increased potential for dawn raids of domestic premises; (ii) inspectors requesting remote access to data stored on (business or personal) devices used for business purposes whilst working from home; (iii) on-the-spot remote questioning of key company personnel (e.g., via video conference); and (iv) (even) shorter raids, since inspectors prefer to copy electronic data on-site but then review this later at the authority's premises.

Preparing your company

Against this background, in formulating an effective internal dawn raid response strategy, companies should already be asking themselves (at least) the following questions:

- Have all staff received comprehensive (and recent) training regarding the company's internal dawn raid response strategy?
    - Do the staff know that their primary objective is to defend the company's interests and legal rights, whilst remaining cooperative with (and not obstructing) the inspectors?
    - Do they know that "obstruction" can in this context be construed very widely and would include not only: (i) "traditional" forms of obstruction such as refusing to speak to inspectors, breaking physical seals and removing/altering/destroying (physical) materials; but also (ii) altering/deleting electronic data (such as emails and WhatsApp chats), or delaying access to IT infrastructure without reasonable excuse?
    - Do they know not to discuss any aspect of the raid with anyone outside of the company?
    - Do they know that there is now an increased chance of: (i) dawn raids of domestic premises; and/or (ii) on-the-spot remote questioning of key company personnel (e.g., via video conference)? Have they received appropriate training to deal with each of these potential scenarios?

- Has a pre-designated internal response team been appointed?
    - Does this include a senior company representative assuming overall responsibility?
    - Does this also include (for example) in-house and/or external lawyers, as well as senior personnel from the company's respective IT, HR, communications and support teams?
    - If the company were to be raided tomorrow, could this team act as an initial point of contact between the company and the inspectors (at least until in-house and/or external lawyers arrive)?
- Do reception and security staff understand the key initial steps they need to take?
    - Do they know to immediately inform a (senior) member of the internal response team (and politely ask inspectors to wait in reception until such person/team arrives)?
    - Do they know to request a copy of the inspection team's authorisation documents, so that the terms/scope of these can be carefully checked (and any concerns quickly raised with in-house and/or external lawyers)?
- Are the company's document management and IT systems (and personnel) ready?
    - Have company systems been updated to prepare for (potentially very extensive) forensic document and data searches?
    - Will senior IT personnel be on hand throughout the raid to manage all IT-related requests from inspectors?
    - Is there a procedure for handling specific requests from inspectors (e.g., to temporarily disable company telephone/email systems and/or to provide remote access to devices used for business purposes whilst working from home)?
    - How long will it take to provide inspectors with full access to company systems (since any unreasonable delay is unlikely to be tolerated)? Are any approvals required for this (and, if so, from whom)?
    - How, where, and for how long are (hard-copy and electronic) documents stored and maintained? Is there a company-wide document management/retention policy (and, if so, how and how quickly can this be suspended in the event of a raid)?
- Has a dawn raid communications strategy been developed?
    - What will staff be told during (and after) the raid? Has the HR team pre-prepared a list of responses to FAQs from staff?
    - What happens if journalists ask the company about the raid?
    - Does the company have disclosure obligations to its insurers and/or auditors (which may differ, if the company is listed)?

- Has the company's internal dawn raid response strategy been stress-tested?
    - Have all staff received comprehensive (and recent) training regarding the strategy, such that they understand exactly what they should/should not do? Are there bespoke guidelines for certain employee groups (e.g., IT and reception)?
    - Would it be helpful to stage a surprise "mock dawn raid" at the company's premises (with appropriate assistance from in-house and/or external lawyers)? Would an audit (or a mini-audit) be more appropriate?
    - How does the internal dawn raid response strategy interact with other company policies (e.g., regarding HR and data protection)? Should any adjustments be made to account for this?

During a dawn raid: some key DOs and DON'Ts	
DO	**DON'T**
• Immediately contact in-house and/or external lawyers, and politely ask inspectors to wait until such lawyers arrive before commencing the inspection (but if the inspectors refuse such request, do not insist on this). • Understand the nature and scope of the raid (e.g., by checking the inspectors' authorisation documents). • Establish a professional relationship with the inspectors (i.e., cooperating with them, and treat them with respect). • Understand the (limits on) inspectors' powers to review and/or copy materials (including those which are potentially irrelevant and/or privileged). • Keep a detailed written record of: (i) all materials reviewed/copied/taken away; and (ii) all questions asked by inspectors (and answers provided by company personnel). • Carefully manage internal and external communications (as well as managing any employees that may be experiencing stress during this period).	• Offer unsolicited information to the inspectors. • Be hostile towards the inspectors. • Obstruct the raid, or the inspectors, in any way (and especially not without first receiving legal advice). • Discuss the fact of the raid (or any aspect of it) with anyone outside of the company.

In the centre of Europe with a global reach

VAN BAEL & BELLIS

Chaussée de La Hulpe 166
Terhulpsesteenweg
B-1170 Brussels
Belgium

Phone: +32 (0)2 647 73 50
Fax: +32 (0)2 640 64 99

vbb@vbb.com
www.vbb.com

5, Chancery Lane
EC4A 1BL London
United Kingdom

Phone: +44 (0)20 7406 1471