

**TO: European Commission
Directorate-General for Competition
Antitrust Registry
B-1049 Brussels
Belgium**

**FROM: XXXXXXXXXXXX
XXXXXXXXXXXX
XXXXXXXXXXXX
ITALY**

Tel. XXXXXXXXXXXX
E-mail: XXXXXXXXXXXX
Web: XXXXXXXXXXXX

13 May 2012

SUBJECT: Monopoly abuse perpetrated by Apple Inc.

My name is XXXXXXXXXXXX and I run an Italian software company as a sole proprietor which develops and sells applications for Microsoft Windows and Apple Mac OS X.

This is to inform you about what I consider a case of monopoly abuse which is going to affect my company in the near future in order for you to start an investigation and take the appropriate actions foreseen by the European and international laws.

I would first of all like to point out that, though Apple Inc. (www.apple.com) is not dominant on the market of operating systems, I firmly believe we are in the presence of an infringement of Article 102 of the Treaty on the Functioning of the European Union (TFEU), which prohibits dominant companies from abusing their position on a particular market. **In fact, the case I am submitting to your attention does not regard an OS monopoly but a monopoly in a certain applications market (the one for Apple OS X systems).**

It is Apple dictating new rules within the previously open applications market for OS X, trying to increase the share of their own sales (they get 30% out of each application sold by third party applications vendors on the Apple App Store). In other words, the two parties involved in this case are **Apple versus third party applications vendors** who are not paying Apple to distribute their software for Mac OS X.

I think that in this case Apple should be considered an applications vendor just like the independent programmers who develop software for Mac OS X **for whom the other operating systems are not an alternative to the one they are currently using** because their applications designed for Mac OS X would not work, for example, on Microsoft Windows or Linux.

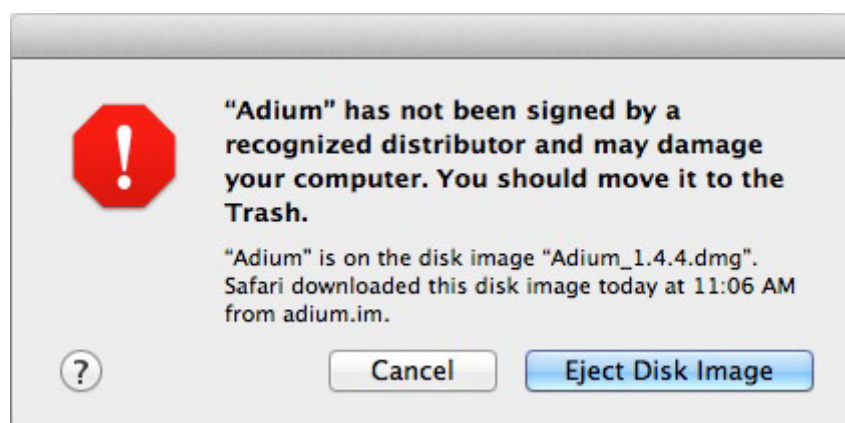
It is indisputable that Apple is dominant on the market of applications for Mac OS X. This market is large enough to be considered **a major commercial reality in itself (there are millions of Mac users)** which, in my opinion, may justify the resort to the European Commission to exclude the existence of any potential infringement of the EU competition rules.

The case of monopoly abuse I am going to submit to your attention regards the way in which Apple Inc. is going to manage the downloads from the Internet of applications for Mac OS X produced by independent software developers like me who have decided not to subscribe to Apple's Mac Developer Program.

Currently, all apps sold through the Mac App Store require **code signing** by Apple and these apps have gone through Apple's review process. For apps sold outside the Mac App Store, code signing is purely optional. It is to be noted that only developers who sign up for Apple's Mac Developer Program and pay the **99 euro/dollar per year fee** can get a code signing certificate called **Developer ID Certificate**.

In the current version of Apple's desktop operating system, **Mac OS X Lion**, launching an unsigned application by double-clicking on its icon brings up a dialog box noting the file was downloaded from the Internet, and asks the user if he or she wants to open it anyway. So, the user who trusts the source only has to click on a button to install the unsigned app.

Unfortunately, things are going to change in Apple's next version of their operating system, **OS X Mountain Lion**, which will be shipped next summer with a new security feature called **Gatekeeper**. Gatekeeper is supposed to protect the users from downloading malicious software by tightly controlling which sources apps can be installed from. **By default**, Gatekeeper will only allow apps from the Mac App Store to be installed, as well as other apps that have been signed using the special ID certificate given to registered OS X developers by Apple. **By default**, Gatekeeper does not offer any option to install an unsigned app when the user double-clicks on its icon. If the app does not pass Gatekeeper's rules, the warning message below pops up to users:



So, if the app is not code-signed, OS X explicitly tells the user to move the app to the Trash and **gives no option to install the app even if the user trusts the source.**

Users can also opt to allow apps from any source but, in order to do so, they have to enter the system preferences and change the default options:



The end result is that inexperienced or average users are not likely to install apps from independent developers who have decided not to sign up for Apple's Mac Developer Program.

According to Apple, OS X Mountain Lion's Gatekeeper is meant to warn users about potentially malicious apps that the user may download from the Web. Nevertheless, with Gatekeeper's default options, Apple is heavily discouraging less experienced users from installing non-Mac App Store apps entirely. I think it is clear that this is one step away from turning the current app freedom on the Mac into the "app dictatorship" of iOS (the operating system for the iPad), where applications can only be downloaded from Apple's App Store.

Becoming a registered OS X developer is onerous for individual developers (e.g. sole proprietors) who would have to pay an annual 99 euro/dollar fee to Apple. Moreover, anyone with a credit card and a working e-mail address can sign up to become a registered developer, so **there is no guarantee that a malware developer has not created and signed an app.** This may demonstrate that the real reason why Gatekeeper will be introduced is **purely commercial.**

Apple stated that if a developer's apps are discovered to be malware, the apps will be registered on a malware list and will be blocked by File Quarantine. The offending developer's ID certificate will also be revoked by Apple, meaning they will not be able to sign any new apps. **Nevertheless, that will not help people who may have installed malware already.**

Furthermore, developers could be penalized if they make an accidental mistake in their programming code in such a way that their application may seem malicious even though it is not. Whenever signed malicious software is encountered, the said certificate is put on the certificate revocation list by Apple and all of the apps produced by that developer will stop working. If there is an appeal, the burden of proof will be the developer's, and nobody is going to compensate his or her losses.

For the above mentioned reasons, I am asking this Directorate-General for Competition to start an investigation and hopefully rule that Apple keep the same system default options which are present in Mac OS X 10.7 (Lion) in the next version of their operating system, OS X 10.8 (Mountain Lion), allowing the user to immediately download unsigned applications after having been informed that they are unsigned.

Yours faithfully,

XXXXXXXXXXXX

XXXXXXXXXXXX