



Commission for  
**Communications Regulation**

## Information Notice

### **PBX Hacking and Telephony Fraud**

<b>Document No:</b>	<b>10/83</b>
<b>Date:</b>	<b>11 October 2010</b>

## Details of Notice

ComReg wishes to advise businesses that there has been a number of recent incidents where business telephone systems have been hacked and businesses have been faced with large bills for calls made over their lines by the people who hack the system. It should be noted that this is not targeted at general consumers as it depends upon a business having its own switchboard or telephone switch system.

Hacking businesses telephone systems/exchanges, known as PABXs (Private Branch eXchange), may result in the company concerned having to pay for the calls that are made by the hackers. These calls can be higher value calls than would normally be dialled by the business thereby exposing the PBX owner to considerable call costs to their network operator. In the space of one or two days businesses can run up bills of tens of thousands of euros as a result of these incidents which arise through poor security procedures being in place for some PABXs in relation to allowing incoming calls to generate external calls through the system.

ComReg understands that these calls often occur when the office of the victim of this fraud is closed and numerous calls are made from the PABX at this time without being detected for some time.

ComReg is now reminding all business PABX users to ensure the appropriate security arrangements are in place for their equipment to prevent hacking for incoming calls. Most equipment of this type will have a number of settings which can be configured to prevent this form of fraud and ComReg would urge businesses to ensure the appropriate security arrangements are in place for their equipment to prevent such hacking and the resulting bills.

### What to do

ComReg recommends that any business that is concerned about this practice should follow these steps:

- Contact your telecommunications provider immediately and advise them of your concerns.
- Contact your PBX supplier (if different from your telecommunications provider) and ensure that your PBX has the latest software updates to prevent unauthorised access and the latest security settings are enabled
- If you suspect that you are a victim of such a crime, contact your local Garda station

ENDS