ReedSmith

Client Alert

Global Regulatory Enforcement

If you have questions or would like additional information on the material covered in this Alert, please contact the author:

Cynthia O'Donoghue
Partner, London
+44 (0)20 3116 3494
codonoghue@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

The European Commission proposes establishing a dedicated European Cybercrime Centre to be situated within Europol, and aims for January 2013 launch date

In a communication from the European Commission to the Council and European Parliament, the Commission proposes establishing a European Cybercrime Centre ("EC3") to be part of Europol to "act as the focal point in the fight against cybercrime in the EU". In its communication, the Commission highlights the total cost of cybercrime to global society as significant, and indicates that no crime is as borderless as cybercrime.

Cybercrime is identified as a high-profit but low-risk form of criminal activity that is becoming increasingly common as we become more of an Internet-based society, using the Internet daily to connect with friends on social networks, or to bank online or do business over the Internet. Cybercrime spans a vast range of offences from identity theft to child sexual abuse to computer fraud and credit card scams which affect EU citizens on a daily basis, and the Commission has recognised cybercrime as a top priority to deal with. Whilst there has been some progress and coordinated efforts to tackle cybercrime, there are still several obstacles to the effective investigation and prosecution of cybercrimes, including tough issues surrounding jurisdictional boundaries, technical difficulties, and inconsistent co-operation and intelligence-sharing between agencies. The aim is that the new EC3 will attempt to tackle these obstacles in the fight against cybercrime.

The EC3 will act as the focal point in the fight against cybercrime in the EU and will form part of the European Law Enforcement Agency, Europol. Europol already deals with computer crimes; however, its resources are limited. The Commission proposes that the EC3 should focus on three key areas:

- Cybercrimes committed by organised crime groups
- Cybercrimes which cause serious harm to their victims
- Cybercrimes which affect critical infrastructure and information systems

However, the Commission recognises that because of the "ever-evolving nature" of cybercrimes, there should be scope for EC3 to take action in response to Member States' requirements and new cybercrime threats.

The Commission highlights the four key functions of EC3 as:

A. To be the European cybercrime information focal point

The aim of this function is to ensure that information is collected about cybercrime from the widest array of public, private and open sources. The information gathered by EC3 would concern cybercrime activities, methods and suspects. Sharing this information would improve knowledge of cybercrime as well as its prevention, detection and prosecution, and will encourage the appropriate links between various relevant authorities. It is hoped this function of EC3 will improve cybercrime reporting and information-sharing, and the Commission suggests that Member States make it a requirement that serious cybercrime offences be reported to the national enforcement authorities in order to pass more information to EC3. One of the main aims of EC3 is to broaden the information picture on cybercrime so that high-profile reports on trends and threats can be produced, and more knowledge around the subject can be gained.

B. To pool European cybercrime expertise to support EU Member States in capacity building

EC3 should assist Member States with expertise and training to curb cybercrime, with the primary focus of the training being on law enforcement. The pooling of resources would also mean streamlining existing initiatives from Europol, CEPOL and individual Member States after a thorough needs-analysis to ensure better co-ordination. The Commission recommends setting up a cybercrime desk to exchange best practice and knowledge, and respond to queries from individual Member States.

C. To provide support to Member States' cybercrime investigations

EC3 should also provide operational support, high-level forensic assistance and encryption expertise for cybercrime investigations.

D. To become the collective voice of European cybercrime investigators across law enforcement investigators

EC3 could potentially act as a rallying point for EU cybercrime investigations, providing a collective voice in discussions with industry, private sector and researchers on how best to prevent cybercrime. EC3 would be the natural interface to Interpol's cybercrime activities and other international cybercrime units, and would collaborate with other organisations to produce public awareness campaigns encouraging safe online behaviour.

The Commission's communication further suggested that EC3 should be part of Europol, and the specific resources required would need to be further assessed, especially in relation to staffing. EC3 should ensure a coordinated response to cybercrime and work closely with Member States, European agencies, international partners, and private sector and research communities.

In order to reach initial operating capability, the Commission is looking to explore, in cooperation with Europol, what is required by EC3 in terms of human and financial resources to

set up an EC3 implementation team until the end of 2013. This team will be established to undertake various tasks, such as drafting the EC3 terms of references and its organisational structure, reaching out to create the first links with the relevant organisations, and establishing a cybercrime desk to be supported by the provision of a dedicated, secure, online community platform.

The establishment of EC3 appears to be a clear demonstration of the Commission's commitment in tackling cybercrime and staying abreast of this fast and ever-evolving form of law-breaking.

ReedSmith

About Reed Smith

Reed Smith is a global relationship law firm with nearly 1,700 lawyers in 23 offices throughout the United States, Europe, Asia and the Middle East. Founded in 1877, the firm represents leading international businesses from FTSE 100 corporations to mid-market and emerging enterprises. Its lawyers provide litigation and other dispute resolution services in multi-jurisdictional and other high-stakes matters; deliver regulatory counsel; and execute the full range of strategic domestic and cross-border transactions. Reed Smith is a preeminent advisor to industries including financial services, life sciences, health care, energy and natural resources, advertising, technology and media, shipping, real estate, manufacturing, and education. For more information, visit reedsmith.com.

Business from offices in the United States and Germany is carried on by Reed Smith LLP, a limited liability partnership formed in the state of Delaware; from the other offices, by Reed Smith LLP of England; but in Hong Kong, the business is carried on by Reed Smith Richards Butler.

Reed Smith LLP is a limited liability partnership registered in England and Wales with registered number OC303620 and its registered office at The Broadgate Tower, 20 Primrose Street, London EC2A 2RS. Reed Smith LLP is authorised and regulated by the Solicitors Regulation Authority. A list of the members of Reed Smith LLP, and their professional qualifications, is available at the registered office and on the website www.reedsmith.com. The term partner is used to refer to a member of Reed Smith LLP or an employee of equivalent standing.

We currently hold your contact details, which we use to send you publications such as this and for other marketing and business communications. We use your contact details for our own internal purposes only. This information is available to our offices worldwide. If any of your details are incorrect or have recently changed, please reply to this email with your new contact details. Or, if you no longer wish to receive publications or other marketing communications from us, please use the opt-out link provided below.

This Alert was compiled up to and including May 2012. It is intended merely to highlight issues and not to be comprehensive nor to provide legal advice. Please refer to this statement for important information on our regulatory position. Should you have any questions on issues reported here or on other areas of law, please contact one of your regular Reed Smith contacts, or contact the authors.