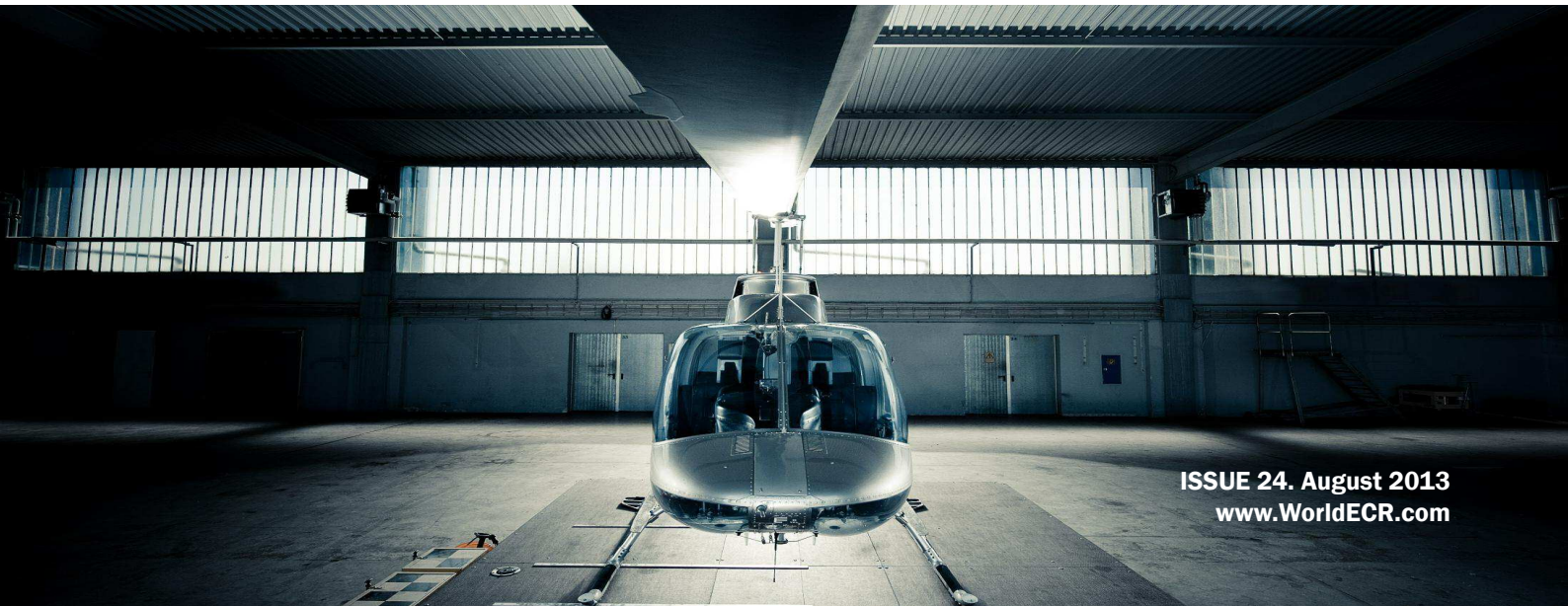
WorldECR



ISSUE 24. August 2013
www.WorldECR.com

Do export compliance clauses serve as a strong enough shield against the U.S. government?

Provisions related to compliance with U.S. sanctions and export controls are regularly to be found in contracts with foreign distributors. But, asks Erich Ferrari, are they worth any more than the paper they are written on?

A number of recent cases have highlighted the difficulties faced by U.S. exporters in ensuring that their products do not end up in the hands of sanctioned parties or jurisdictions. For example, on 3 May, the *New York Times* reported that Dell computer equipment, including hundreds of laptops, tablets and desktop computers, has ended up in the hands of the Syrian government by way of a UAE-based re-exporter. According to the *Times* report, Dell computer equipment was sold to BDL Gulf, a major distributor of computer equipment in the Middle East and Africa, and one of Dell's authorized dealers. From there, an employee of BDL arranged the sale of the equipment to Syria-based Anas Hasoon Trading Company, despite the fact that the company's representative made it clear that the equipment was intended for use by the Syrian government.

Blue Coat Systems

Incidentally, the article describing the Dell incident came out shortly after a $2.8 million fine was assessed by the Department of Commerce's Bureau of Industry and Security ('BIS') against a different UAE-based distributor for providing equipment designed to monitor and control web traffic to the Syrian government. That equipment was manufactured by U.S.-based Blue Coat Systems.

In the Blue Coat case, the internet 'hacktivist' group Telecomix released information which indicated that two Blue Coat products, the Blue Coat Proxy SG 9000 system and the K9 Web Protection filtering system, were being used by the Syrian government. Soon after the reports surfaced, both Blue Coat and BIS initiated investigations into the matter. Within two months, BIS added Wassem Jawad and the Ras Al Khaimah-based company Info Tech to its entity list, which restricts the export of items that fall under U.S. jurisdiction to persons contained therein. According to BIS, Jawad was responsible for purchasing the Proxy SG 9000 systems from a then-unnamed authorized Blue Coat distributor for the Syrian government. At the time, Under Secretary for Industry and Security Eric L. Hirschhorn warned that 'additional enforcement actions are likely'.

After further investigation, BIS charged Computerlinks FCZO, Blue Coat's distributor in the UAE, with violations of the Export Administration Regulations. It alleged that Computerlinks deliberately provided Blue Coat with false end-user data, stating that the devices were bound for the Iraqi and Afghan governments, which did not require a licence in this particular instance. The systems eventually ended up in the hands of Syrian Telecommunications Establishment. Under the terms of the settlement, Computerlinks was assessed a $2.8 million fine, which it was required to pay before being granted any additional export licences. In addition, Computerlinks was required to perform three external audits of its export controls compliance programme. Despite all of this, Blue Coat has yet to suffer any consequences as a result of the violations.

Movement beyond control

The Dell and Blue Coat cases display the ease in which U.S.-origin goods can end up in the hands of sanctioned entities or jurisdictions despite the best efforts or intentions of the original exporter. As part of their efforts to prevent such occurrences, U.S. exporters, particularly those dealing in sensitive technology, typically include provisions related to compliance with U.S. sanctions and export controls in their contracts with foreign distributors. These can include detailed descriptions of compliance requirements and often specifically reference prohibitions on sales to restricted end-users or jurisdictions. Indemnity clauses are also necessary in the event that a re-exporter violates these terms.

For example, in accordance with the terms of its distribution agreement with Blue Coat, Computerlinks FCZO was required to 'comply with all export and import laws, rules, policies, procedures, restrictions, and regulations of the Department of Commerce'. Moreover, on its website Blue Coat specifically states that 'Exports to companies, organizations, or persons listed on the Specially Designated Nationals List, the Debarred List, the Entity List, and other governmental lists are prohibited.'

For its part, Dell also mandates that any re-export of Dell products comply with relevant export controls. Under its Terms and Conditions for Resellers[1] 'Products shipped pursuant to this agreement may not be sold, leased or otherwise transferred to restricted end-users (including those on the U.S. Department of Commerce, Bureau of Industry and Security "Entity List" and other lists of denied parties) or to restricted countries (currently Cuba, Iran, North Korea, Sudan, and Syria).' It also contains an indemnity clause in the event that the reseller violates any applicable export controls, including a specific reference to any 'investigations or proceedings by a governmental agency or entity'.

The mere presence of these contractual provisions obligating third-party re-exporters to comply with applicable export controls does not in

Links and notes

[1] http://www.dell.com/learn/us/en/19/terms-of-sale-reseller

[2] While the incidents discussed in this article relate to exports to Syria, the idea is the same; namely that Szubin's comment referenced exports to a country subject to export controls and/or sanctions.

and of itself remove a U.S. manufacturer's liability, however. As the Director of the United States Department of the Treasury's Office of Foreign Assets Control ('OFAC') Adam Szubin warned in 2009, 'It is reasonable for us to ask, what have you done to make sure your export doesn't go to Iran… We won't countenance willful blindness.'[2]

ICP should be robust

OFAC's enforcement guidelines also make clear that exporters are expected to maintain a robust risk-based compliance programme, particularly when dealing with re-export hubs such as those in the UAE. For example, in determining whether an enforcement response is warranted in response to sanctions violations, OFAC specifically considers whether the subject of the investigation had 'reason to know' or could have 'reasonably known based on all readily available information and with the exercise of reasonable due diligence, that the conduct would or might take place'. BIS's compliance guidelines take a similar position, stating that 'an affirmative policy of steps to avoid "bad" information would not insulate a company from liability, and it would usually be considered an aggravating factor in an enforcement proceeding.'

Thus, the aforementioned export compliance clauses are a starting point, but not an absolute shield to liability. Case in point: in February 2012, OFAC fined California-based Teledyne Technologies $30,385 for violating the Sudanese Sanctions Regulations related to the indirect export of acoustic doppler current profilers. This penalty came despite the presence of the re-export control requirements and a voluntary self-disclosure of the violations to OFAC.

It is therefore essential that U.S. exporters ensure that they take steps to ensure that their resellers are in compliance. This should include affirmative steps to educate foreign distributors about their export control responsibilities and the potential penalties that could be incurred should violations occur. This not only ensures the durability of any exporter-distributor relationship, but mitigates the significant reputational costs associated with public disclosures of sanctions violations. While Blue Coat may have avoided any administrative penalties itself, it certainly would have preferred that its brand not be associated with the domestic surveillance activities and human rights violations of the Syrian government.

From the *Times* report, it is clear that Dell has a great deal of work to do. According to BIS best practices regarding dual-use goods, 'companies should obtain information about their customers that enables them to protect dual-use items from diversion, especially when the foreign customer is a broker, trading company or distribution center.' Despite this recommendation, when asked about the origins of the company's customers, BDL Gulf's sales manager for the UAE, Africa, and Iran responded, 'We cannot know if they are from Pakistan, Egypt or Morocco; we just sell in Dubai.' Exporters should be extremely wary of such distributors who fail to perform even the most rudimentary know-your-customer ('KYC') checks.

The mere presence of these contractual provisions obligating third-party re-exporters to comply with applicable export controls does not in and of itself remove a U.S. manufacturer's liability.

Furthermore, after funds transfers from Syrian banks were rejected by Dubai banks because of sanctions, the Syrian company's representative directed cash deposits into BDL's account to pay for the Dell products, itself another obvious red flag. While emails shown to the *Times* indicated that the BDL sales manager in question was aware that the products were in fact destined for Syria, the fact that the illicit nature of the transactions were not flagged by others at BDL demonstrates doubt regarding the effectiveness of the company's current compliance measures.

Extraterritorial jurisdiction

In addition to the above, the Computerlinks FCZO settlement is also indicative of how both BIS and OFAC assert extraterritorial jurisdiction. A number of sanctions programmes, including the Syria Sanctions Regulations, Iranian Transactions and Sanctions Regulations, and the Cuban Assets Control Regulations, contain prohibitions on the re-exportation of U.S.-origin goods, technology, and services by non-U.S. persons if the transaction would have been prohibited if undertaken by U.S. persons. Therefore, even non-U.S. re-exporters may be required to obtain licences from both OFAC and BIS for products which fall under the following guidelines:

- The goods were produced or originated in the United States;
- The goods are a foreign-made product that contains more than a specified percentage of U.S.-controlled content, either 10% or 25% depending on the ultimate export destination;
- The goods are a foreign-made product based on certain U.S.-origin technology or software and are intended for shipment to specified destinations;
- The goods were made by a plant or major component of a plant located outside the United States, and if that plant or major component of a plant is the direct product of certain U.S. technology or software, and the product is intended for shipment to specified destinations.

That said, what these and other similar cases tend to show is that so long as appropriate due diligence measures are in place, neither OFAC nor BIS is interested in targeting exporters for the sins of their distributors. So any Apple executives who happened to be watching the recent presidential debates can rest easy knowing that the iPad used by former Tehran Mayor Mohammad Qalibaf is unlikely to result in an investigation, especially considering the recent general licence authorizing the sale of certain electronics and communications equipment to Iran.

Erich C. Ferrari is a partner at Washington, DC firm Ferrari & Associates, P.C., where he advises on sanctions and national security issues.

ferrari@ferrariassociatespc.com

This article is reprinted from the August 2013 issue of WorldECR, the journal of export controls and sanctions.

WorldECR

The journal of export controls and compliance

Contributors in this issue

Erich C. Ferrari, Ferrari & Associates, P.C.
www.ferrariassociatespc.com

Larry E. Christensen and David Hardin,
Miller & Chevalier
www.milchev.com

Daniel Martin, Holman Fenwick Willan LLP
www.hfw.com

Laurent Ruessmann and Jochen Beck,
Field Fisher Waterhouse LLP
www.ffw.com

Clifford Sosnow and Sean McGurran,
Fasken Martineau DuMoulin LLP
www.fasken.com

Ivo Janda, White & Case LLP
www.whitecase.com

General enquiries, advertising enquiries, press releases, subscriptions: info@worldecr.com

Contact the editor, Tom Blass: tnb@worldecr.com tel +44 (0)7930405003

Contact the publisher, Mark Cusick: mark.cusick@worldecr.com tel: +44 (0)7702289830

WorldECR is published by D.C. Houghton Ltd.

ISSN 2046-4797. Refer to this issue as: WorldECR [0304]

Correspondence address: D.C. Houghton Ltd, Suite 17271, Lower Ground Floor, 145-157 St John Street, London EC1V 4PW England

D.C. Houghton Ltd is registered in England and Wales (registered number 7490482) with its registered office at 145 - 157 St John St, EC1V 4PY, London, UK

ISSUE 24. AUGUST 2013
www.WorldECR.com