PaymentsCompliance

OFAC Warns Of Crimea Payment Processing Sanctions Risks

7TH AUG 2015 | WRITTEN BY:MARK TAYLOR

U.S. financial intelligence units have issued guidance on how to mitigate risks of processing payments linked to Crimea and avoid violating sanctions placed on Russia.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is stepping up enforcement of the Russia sanctions regime, and has advised payment and financial services to assess their risks.

It has issued a clarification on the "misunderstood" nature of the embargo to U.S. businesses, and foreign entities conducting business through the United States.

Techniques used to exploit this misunderstanding have been highlighted in the guidance.

Sanctions were placed on Russia after military forces annexed the region of Crimea from Ukraine last year.

Of concern is Executive Order 13685.

This prohibits "virtually all direct and indirect transactions (including financial, trade, and other commercial transactions) by U.S. persons or within the United States to or from Crimea unless authorized by OFAC or exempted by statute."

The evasive practices identified by OFAC include the omission or confusion of references to Crimea and locations within Crimea in documentation underlying transactions involving U.S. persons or the U.S.

These practices apply to a range of activities in the financial services.

The guidance states: "It is important to note that Crimea is not a country; rather it is a geographic region located in southeastern Ukraine bordering the Black Sea.

"Crimea is a geographical region, and will typically not appear by name in payment instructions, letters

of credit, or trade documents.

"It is therefore imperative that U.S. businesses screen locations within the Crimea region, to include cities, towns and ports.

"Like all other sanctions programs, businesses should take a risk-based approach to compliance with this embargo."

OFAC said it had become aware that certain individuals or entities have been engaged in a pattern or practice of repeatedly omitting originator or beneficiary address information from Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages.

This involved individuals ordinarily resident in, or entities located in, Crimea.

In response to the sanctions regime, Russia created its own domestic payments network to avoid being cut out of international transactions by Visa and MasterCard.

Financial expert Burt Braverman, a partner at the Washington office of Davis Wright Tremaine law firm, said: "OFAC reported that financial institutions discovered the data missing from these SWIFT messages through enhanced due diligence efforts performed on one of the transaction parties after identifying a suspicious Crimea-related pattern or practice."

He said the enforcement agency would not look favourably on any company pleading innocence, adding that companies operating in the financial services sector should heed OFAC's warning "given the potential severity of penalties."

"Persons and entities operating in the financial services and international trade sectors would be well-advised to take note of OFAC's warnings and suggestions," he said.

"OFAC previously has imposed significant penalties under other sanctions programs on persons, companies and financial institutions that engaged in or facilitated, either knowingly or through disregard for sanctions compliance obligations, similar obfuscating practices, such as omission or truncation of identifying information from SWIFT messages.

"Having issued the advisory, claims of inadvertence or ignorance of the Crimean sanctions requirements will not be well-received by OFAC as mitigating factors in the penalty phase of an enforcement action."

The risk of processing transactions in apparent violation of OFAC sanctions on Crimea can be mitigated by implementing the following types of measures:

- Ensuring transaction monitoring systems include "appropriate" search terms corresponding to major geographic locations in Crimea and not simply references to "Crimea".
- Requesting additional information from parties, including financial institutions, corporate entities,

and individuals, that previously have violated or attempted to violate U.S. sanctions on Crimea. Such prior conduct could include, for example, routing transactions to or through U.S. financial institutions with inaccurate or incomplete address information for Crimean individuals or entities.
- Clearly communicating U.S. sanctions obligations to international partners and discussing OFAC sanctions compliance expectations with correspondent banking and trade partners. This could include a description of the prohibition on the direct and indirect exportation or re-exportation of goods, technology, and services (including financial services) from the U.S. to Crimea.

OFAC notes the above are merely examples of steps that can be taken to mitigate risks and companies "should tailor specific compliance measures to their own risk profile".

In March, OFAC handed PayPal a $7.7m fine for failing to employ adequate screening procedures.

The Californian processor approved payments for individuals involved in the illicit handling of weapons of mass destruction (WMD) and international drug smuggling, ignoring its own warning signs and not acting on a chance to notify the government.

Topics: E-COMMERCE

Geography: UNITED STATES, EUROPE, RUSSIA

Sectors: CARDS, CREDIT, DEBIT, DIGITAL PAYMENTS, PAYMENT PROCESSING, CROSS-BORDER PAYMENTS, RETAIL, GAMBLING

Content: NEWS & ANALYSIS