Latest news on the draft cyber security law for Jersey

Insights - 11/03/2024

The prime strategic threat to Jersey as a leading international finance centre is financial crime.

This was the view shared by Jonathan Groom MBE, director of the Financial Intelligence United for Jersey (**FIU**) in his opening address at the FIU's recent partnership and collaboration event.

In the Government of Jersey's National Risk Assessment, the most recent update for which was published in September 2023 (**NRA**), it identified that Jersey represents 1.35% of the global market for cross-border financial services. The importance of the banking and financial services sector, including legal and accountancy services, to Jersey's economy cannot be overstated – in 2021, it accounted for some 37.5% of Jersey's total Gross Value Added output and 22% of employment.[1]

Financial crime and cyber crime go hand in hand – gone are the days when hard currency was the medium of exchange of choice in the developed world, with the vast majority of banking and financial services now being conducted electronically. This includes both the transactions themselves and the associated records. It follows that measures to protect cyber security are needed to adequately protect these transactions and records.

It is unsurprising, on this basis, that providers of banking and financial services have been classified as one of the Operators of Essential Services (**OES**) in the new draft Cyber Security (Jersey) Law, the White Paper for which was put out for consultation by the Government of Jersey on 4 March 2024 (**the draft law**).

Matthew Shaxson (co-chair of Ogier (Jersey) LLP's Regulatory Group), **Tom Hall** (senior associate, Ogier (Jersey) LLP), and **Andy Carpenter** (senior consultant, Ogier Regulatory Consulting) explore the draft law and its implications for banks, trust company service providers and fund services businesses providing a service of that kind in Jersey, which we will refer to as **Banking and Financial Service Providers**.

What does the law propose?

The draft law proposes, in brief terms, a number of new measures to protect against the cyber crime threat to OES by addressing the cyber security measures that they are expected to adopt. It also proposes the establishment of a new Jersey Cyber Security Centre, Commissioner for Cyber Security and Technical Advisory Counsil to advise the Commissioner.

To qualify as a banking or financial services OES, an entity needs to:

1. either be providing banking and credit services (registered under Part 2 of the Business Banking (Jersey) Law 1991, and regulated by the Jersey Financial Services Commission (**JFSC**)) or providing financial service business (as defined by Article 2 of the Financial Services (Jersey) Law 1998 and regulated by the JFSC). The definition of "financial service business" in particular is broad, and covers any "person" carrying on (amongst other things) investment business, trust company business, general insurance mediation business, money service business and fund services business; and
2. provide those services in reliance upon network and information systems (there is, unlike the provision of services by some other OES, no minimum value threshold applicable to those services [2]).

In practice, this is likely to encompass all Banking and Financial Service Providers.

The draft law requires all such businesses to give notice to the Minister within 28 days of the draft law coming into force.[3] Where the OES in question has its head office outside Jersey, it will need to nominate an authorised person in Jersey to act on their behalf.[4]

The OES will then be under a duty to:

"...implement measures that are appropriate and proportionate for the purposes of -

- *identifying cyber threats to the security of the network and information systems on which the provision of their essential service relies;*
- *reducing the risk of incidents affecting the security of those network and information systems occurring;*
- *preparing for the occurrence of such incidents, and preventing and minimising their impact; and*
- *ensuring the continuity of their essential service".**[5]***

It is noted that the measures implemented must ensure a level of security of network and information systems appropriate to the cyber threat and risk posed.[6] The Minister may require an OES to take further specified measures that they consider are appropriate and proportionate.[7]

What happens in the event of a cyber incident?

In the event of a cyber security incident, the OES is under a duty to notify the Commissioner for Cyber Security (which will be established pursuant to the draft law), inform service users and take any steps mandated by the Minister in response to a significant cyber security incident and the adverse effects of that incident[8].

A new offence is created where a person knowingly or recklessly provides a "relevant person" with false or misleading material in purported compliance with a requirement under the draft law or in circumstances where they intend, or could reasonably be expected to know, that the information would be used for the purpose of carrying out their function. A "relevant person" in this context includes the Minister, the Commissioner, the Jersey Cyber Security Centre and any other person entitled to information under the draft law.[9]

It is also noteworthy that any information shared with the Commissioner in the exercise of their function may be shared by the Commissioner, if they consider it to be in the interests of security of Jersey or for the purposes of prevention or detection of crime or investigation of an offence, with law enforcement authorities and any other person the Commissioner considers appropriate. They may also assist in investigations by other bodies, such as the JFSC, the Information Commissioner, the States of Jersey Police and the Jersey Competition Regulatory Authority.

Whilst many Banking and Financial Service Providers will already have in place robust measures to prevent cyber security breaches and financial crime in order to comply with their anti-money laundering, legal and regulatory duties, there are a few particular points of note:

1. The draft law proposes enhanced administrative obligations on OES's and places them under an obligation to keep appropriate and proportionate measures in place to identify, prepare for and reduce the risks of cyber crime.

What is "appropriate and proportionate" is not defined in the draft law. It will likely be a fact-specific assessment on a case by case basis. Relevant factors might include the amount of business conducted by the Banking and Financial Service Provider (by volume and value) and the size and resources of the Banking and Financial Service Provider. If the measures are not deemed to be adequate, the Minister can specify further measures to be taken by the OES.

It is also noteworthy that it is proposed that the Commissioner will be given powers to set or adopt standards in relation to cyber security which the affected persons should then apply.

Rather than being viewed as a burden, this should be viewed as the part of the important role that industry plays in combatting cyber and financial crime.

2. In acknowledging the importance of maintaining appropriate and proportionate measures to identify and protect against cyber crime, this continues the developing trend towards

implementing technological solutions to meet these obligations. An example of this is the JFSC's Innovation Hub, a recently founded body to allow the JFSC to work with industry and technology companies to implement Fintech, Regtech and Suptech developments, ultimately aimed at reducing the burden on both obliged person and regulator whilst improving the quality of information flow.

3. The fact that information sharing between "relevant persons" and the power to assist in investigations is expressly provided for in the draft Law is a further example of the ongoing attempts to further enhance collaboration between regulatory, intelligence and law enforcement bodies.

What happens next with the proposed law?

The consultation window is only open for a limited period of time, closing on 23 April 2024, having previously only been open until 19 March 2024. One assumes that the extension is to provide further opportunity for prospective OES to make their views on the draft Law known to the Jersey Government, who will then look to consider any comments arising from the consultation, with a view to laying it before the States as soon as practicable. It will be interesting to see what response is received from industry, and whether the draft law is subject to amendments or broadly enacted as drafted.

For example, the ability exists for an OES to appeal against its designation as such. It stands to reason that certain industries may respond to the consultation questioning whether they ought to be designated as an OES or, if they are, what the appropriate *de minimis* level (above which they are deemed to be an OES) ought to be. Given the importance of the banking and financial services industry to Jersey, it seems likely that the banking and financial services industry will remain on the list of OES's.

If you have any questions about the draft cyber security law, please do not hesitate to contact our team via their contact details below.

[1] Source – Government of Jersey National Risk Assessment, September 2023

[2] Article 24 and Part 3 of Schedule 3 of the draft Law

[3] Article 24(3) – (4) of the draft Law

[4] Article 26 of the draft Law

[5] Article 29 of the draft Law

[6] Article 29 of the draft Law

[7] Article 30 of the draft Law

[8] Articles 31 – 33 of the draft Law

[9] Article 36 of the draft Law

About Ogier

Ogier is a professional services firm with the knowledge and expertise to handle the most demanding and complex transactions and provide expert, efficient and cost-effective services to all our clients. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

Key Contacts

Matthew Shaxson

Group Partner, Ogier Legal L.P.

Jersey

E: matthew.shaxson@ogier.com

T: +44 1534 514064

Tom Hall

Managing Associate

Jersey

E: tom.hall@ogier.com

T: +44 1534 514443

Andy Carpenter

Senior Consultant - eDiscovery and Digital Forensics

Jersey

E: andy.carpenter@ogier.com

T: +44 1534 514492

Related Services

Crypto Disputes

Ogier Regulatory Consulting

Cyber security consulting

Related Sectors

Technology and Web3