CAYMAN ISLANDS
MONETARY AUTHORITY

To: All Licensees

From: Cayman Islands Monetary Authority

Date: 25 May 2016

Cybersecurity

Earlier this year, the Cayman Islands Monetary Authority reminded the financial services industry that Licensees should remain focused on their organization's data security, given the persistence of threats as cybersecurity issues continue to rise globally. Over recent months the vulnerability of entities operating in International Financial Centers, such as the Cayman Islands, has been heightened, as has the consequences of security breaches. The objective of this Circular is to further raise the level of awareness and to encourage licensees to re-assess their strategies.

The Authority sees cyber-attacks as one of the key risks that the financial sector faces in today's digital environment, where much reliance is placed on mobile computing technologies and the Cloud, presenting increased opportunities for cyber criminals. Cyber-attacks are much more frequent, they have become extremely sophisticated and as institutions around the globe are finding, they are very costly.

Today's Financial Institutions are being increasingly targeted by hackers who are using extremely sophisticated methods to break into their systems. Financial Institutions are having to respond with robust security systems to avoid business interruption, financial losses and reputational damage. *PWC's 2016 Global State of Information Security Survey* found that in 2015, 38% more security incidents were detected than in 2014. It was also noted that the average security budget across industries increased by 25%. The most significant cybersecurity challenges identified in the PWC report were:

1. Security protocols/standards of third-party vendors
2. Rapidly evolving, sophisticated, & complex technologies
3. Cross-border data exchanges
4. Increased use of mobile technologies by customers; and
5. Heightened information security threats from outside the country

Given the heightened risk, the Authority is reviewing and strengthening its own security strategy. Along with Central Government and the Information and Communication Technology Authority ("ICTA"), the Authority has taken the decision to adopt the National Institute of Standards and Technology Cybersecurity Framework, which is a risk-based set of guidelines designed to help organizations assess current capabilities and create a prioritized roadmap towards improved cybersecurity practices. The Authority is working to establish a set of internal policies and procedures to implement the Framework, which is a reiterative process designed to keep abreast of new threats, processes and technologies. The standard identifies five core functions of effective cybersecurity which are: Identify, Protect, Detect,

Respond, and Recover. Creation of detailed procedures and policies to cover each of these areas will provide the Authority with the enhanced tools necessary to operate in today's digital environment while being prepared to respond to a cyber event.

As the Authority works closely with the ICTA and the Financial Crimes Unit, we are well aware of the escalating attacks targeted directly at the Cayman Islands in general and our financial industry in particular. While the Authority recognizes that many of our licensees have robust data security systems, we also recognize that there may be others that may have systems that are improper or inadequate. The Authority is therefore strongly encouraging licensees to assess their cybersecurity risks, reassess their strategies to ensure they are comprehensive and up-to-date for the current environment and to test their security programs to identify vulnerabilities to their systems.

As noted in our first *Supervisory Issues and Information Circular* issued in February, going forward, the Authority will review licensees' approaches to data security risk management. Depending on a licensee's business and risk profile, we will examine one or more of the following areas: technical controls, incident response, and staff training. As part of our reviews, the Authority will also consider licensees' ability to protect the confidentiality, integrity and availability of sensitive customer and other information.