150 SOCIAL MEDIA RISK MANAGEMENT

Policy statement. BSFIs shall comply with the foregoing standards on social media risk management within a period of six (6) months from 04 April 2017. In this regard, a BSFI should be able to show, upon request of the Bangko Sentral, its plan of actions with specific timelines, as well as the status of initiatives being undertaken to fully comply with the provisions of this Section.

Social media, a low-cost solution capable of disseminating real-time information via the internet, presents vast opportunities for growth, customer engagement and business benefits as usage, customer reach and adoption scale up and become widespread and ubiquitous. Considering these potential benefits alongside exponential growth in the number of social media users and its massive reach, BSFIs have started to leverage on social media platform/s to promote their business and improve customer interaction experience to help drive business objectives/strategies.

Similar to any new technology, however, social media introduces a new attack vector which may expose BSFIs to compliance, legal, reputational, strategic, and operational risks. Risks in social media include susceptibility to account take-over, malware distribution, brand bashing, inadvertent disclosure of sensitive information and privacy violation, among other possible threats. As such, BSFIs should adopt an appropriate risk management system, commensurate with the extent and degree of their social media usage, to effectively identify, measure, manage and monitor risks arising from the use of social media platforms. This should form an integral part of their operational risk management system.

Applicability and scope. The guidelines underscore the importance of having a well-defined social media risk management strategy in supporting BSFI's overall business goals and objectives. These guidelines align existing regulations, to the extent possible, with leading standards and recognized principles. They outline the minimum standards/basic principles that shall govern the BSFI's framework to aid in the sound management of risks associated with the use of social media for official purpose or employees' personal use, within and outside the organization.

It is not intended to provide procedural specifics or a "one-size-fits-all" solution for carrying out compliance and risk management responsibilities. Each BSFI is therefore expected to establish its own risk management strategy; suitable to its size, risk tolerance level, and the nature and scope of social media activities engaged in.

The guidelines shall apply to all BSFIs which include banks, NBQB, non-bank electronic money issuers, and other non-bank institutions which under existing Bangko Sentral rules and regulations and special laws are subject to Bangko Sentral supervision and/or regulation.

Definition of terms. In these guidelines, terms are used with the following meanings:

a. *Attack vector* shall refer to the path or means by which an attacker can gain access to a computer system in order to deliver a malicious code (e.g., virus, worms, trojans).

b. *Non-technical controls* shall refer to management, administration, and operational controls employed that are manual and procedural in nature (e.g., security-related policies and procedures; operational procedures; personnel, physical, and environmental security controls; performance management and measurement).

c. *Risk assessment* shall refer to the process involving the identification and assessment of potential threats and vulnerabilities related to the use of social media and determination of the likelihood that the threat will occur as well as the corresponding impact to the business should the threat occur.

d. *Social media* shall refer to online communication channels dedicated to community-based content generation and sharing, interaction, and collaboration.

e. *Social media platform* shall refer to any form of interactive communication medium wherein users can generate and disseminate content (e.g., text, images, audio, video) through social networks using the internet. Examples of popular social media platform categories include the following:

(1) Social networking (e.g., Facebook, Linkedln)
(2) Micro-blogging (e.g., Twitter, Tumblr)
(3) Blogging (e.g., WordPress, Blogger)
(4) Photo Sharing (e.g., Flicker, Instagram, Pinterest)
(5) Video Sharing (e.g., Youtube, Vimeo, Vine)
(6) Crowdsourcing (e.g., Ushahidi, Inc.)

f. *Technical controls* shall refer to the controls incorporated into the computer hardware, software, or firmware to aid in the effective implementation of policies and standards (e.g., access control, authentication, web scanner/crawler).

Social media risk management system. BSFIs should establish an appropriate framework that will result in sound social media governance and risk management. At a minimum, the framework shall include the following elements:

a. Clearly defined governance structure indicating the roles and responsibilities of the board of directors and senior management in setting the direction on the BSFI's use of social media, including its alignment to the BSFI's strategic goals/plans; establishing adequate standards, policies, procedures, and controls; and implementing ongoing risk assessment of social

media-related activities.

The board of directors shall be primarily responsible for defining the BSFI's risk tolerance level, understanding the nature and degree of risks the BSFI will be exposed to, and ensuring that these risks are properly addressed. Moreover, the board of directors, as part of its duties, shall approve and oversee the design and implementation of the social media strategy; related standards, policies and procedures; and means to ensure compliance with said standards and/or policies as well as applicable laws and regulations. Senior management, on the other hand, shall be responsible for the implementation of the social media risk management system approved by the board of directors.

The governance process should also include reporting mechanisms to the board of directors and/or senior management to enable periodic evaluation of the effectiveness of the BSFI's social media strategy/program, in terms of achieving its stated objectives, and measures put in place to manage the risks related to its use.

b. Policies and procedures governing the following, among others:

(1) Scope and definition of social media;

(2) Social media regulatory landscape reflecting applicable laws, rules and regulations for compliance;

(3) Individuals and/or composition of the team/s who will be responsible for the creation, maintenance, and monitoring of the BSFI's proprietary social media sites/pages. Their corresponding roles and accountabilities should also be clearly defined;

(4) Content management and approval process;

(5) Ongoing assessment, management, and monitoring of risks associated with social media-related activities;

(6) Acceptable use as well as prohibitions/restrictions on the business/official use of social media platforms. These guidelines shall likewise apply to the employees' [1] personal use of social media, insofar as it may impact the BSFI's operations, reputation and/or compliance with applicable laws and regulations. These should cover matters such as, but not limited to, expectations, ethical behavior, types/nature and extent of BSFI and/or customer-related information that can be posted, statements that can or cannot be made about or in behalf of the institution, comments that should not be made about a competitor, and corresponding

sanctions/penalties for inappropriate use of social media and committing non-permissible activities;

(7) Use and monitoring of the BSFI's proprietary social media sites/pages to ensure compliance with applicable laws, regulations and internal policies;

(8) Monitoring and recording of suspicious transactions and customer activities on the BSFI's proprietary social media sites/pages;

(9) Adoption of technical and non-technical controls to address risks associated with the use of social media platform/s including methodologies to manage risks from online postings, edits, replies and retention;

(10) Due diligence process for selecting, managing and continuous monitoring of third-party service providers (TSP) that administer the BSFI's social media site(s)/page(s). In addition, the specific roles and responsibilities of the TSP, including liabilities and accountabilities for errors, omissions, fraud, and other instances, resulting from the TSP's actions, which may adversely affect the BSFI, should also be defined;

(11) Social media crisis management plan and escalation procedures;

(12) Enterprise-wide employee training and awareness programs covering relevant topics such as the BSFI's social media use policies, employee roles and responsibilities and non-permissible activities;

(13) Records retention of social media data; and

(14) Communication of the BSFI's official social media sites/pages to its customers to avoid confusion and being misled to unofficial sites.

c. Specific roles and responsibilities of the risk management, consumer protection, audit and compliance functions to ensure that social media risks are adequately managed and integrated in the BSFI's enterprise-wide risk management systems.

BSFIs that do not utilize social media should nevertheless have clear policies and measures in place to address the potential reputational risks that may arise within the various social media platforms and provide guidance on employee use of social media.

Compliance with relevant regulations. BSFIs, in formulating and implementing their social media

policies, should ensure compliance with the applicable requirements of Bangko Sentral rules and regulations on financial consumer protection, especially those relating to disclosures and transparency in advertising and promotional materials, protection of client information, effective recourse, and financial education and awareness. They should likewise conform to the relevant provisions of Bangko Sentral outsourcing framework should they decide to outsource the conduct of social media-related activities to a service provider.

The use of social media platforms, including information gathered therein, for the conduct of account origination activities should comply with applicable rules and regulations, especially on the provisions relating to customer identification procedures under the existing anti-money laundering rules and regulations. In the event that BSFIs opt to use social media for processing financial transactions, the applicable Bangko Sentral rules and regulations on electronic banking/electronic services and technology risk management should likewise be observed to ensure security, reliability and authenticity of such transactions.

The regulations mentioned herein are not exhaustive. It is the BSFI's responsibility to ensure that all applicable laws and regulations relevant to the activities it will choose to engage in using social media will be adequately complied with. Moreover, the BSFI is expected to stay abreast of and continuously adapt to changes in the regulatory requirements.

Supervisory enforcement actions. BSFIs should make available all policies and procedures and other documents/information related to the foregoing during the on-site examination as well as provide copies thereof when a written request is made to determine compliance.

Consistent with Sec. 002, the Bangko Sentral may deploy enforcement actions to promote adherence with the requirements set forth in Sec. 150 and bring about timely corrective actions. The Bangko Sentral may issue directives to improve the social media risk management system or impose monetary and non-monetary sanctions on a BSFI and/or its directors, officers and/or employees.

(Circular No. 949 dated 15 March 2017)

Footnotes

1. Includes the BSFI's employees, contractual employees and/or project hires, and third-party service providers