CIRCULAR **NSE/RD/BDR/CIR9/20/05/15**

15 May 2020

Circular to Dealing Members on Cyber Security Threats, Business Continuity and Fraud Prevention

The COVID-19 pandemic has had unprecedented, far reaching, and damaging effects on a global scale. The Exchange notes the extent of this disruption to our stakeholders, particularly on the Dealing Member community and the Nigerian capital market. In response, we implemented our Business Continuity Plan which enabled Dealing Members to trade remotely and seamlessly using The Exchange's FIX Protocol services and Virtual Private Network (VPN) access.

Dealing Members have made considerable efforts to manage the impact of the pandemic by leveraging on technology to execute customer mandates and connect with internal and external stakeholders. However, the increased use of work from home arrangements and virtual teleconferencing has led to an increased risk of cyber-attacks arising from impersonation, phishing scams, ransomware, business electronic mail compromises, and other attacks.

While Dealing Members are understandably focused on business resilience and the health and safety of their employees and clients, it is important that firms remain vigilant in their surveillance against cyber threats and take steps to reduce the risk of cyber incidents.

This circular outlines measures, though not exhaustive, that firms should take to address increased vulnerability to cybersecurity attacks and to protect customer and firm data on firm and home networks, as well as on devices.

A. Steps to Mitigate Cybersecurity Attacks

1. Use a secure network connection to access your firm's work environment (*e.g*. through a company-provided Virtual Private Network (VPN) or through a secure firm or third-party website (which begins with "https"). Please note that https is an acronym for Hypertext Transfer Protocol Secure, which is the secure version of Hypertext Transfer Protocol (HTTP) used to send data between a web browser and a website. Use of HTTPS is recommended for all websites to ensure secure communication over computer networks;
2. Ensure endpoint protection on all laptops and mobile devices, including Virtual Private Network (VPN) tools with encryption. Endpoint encryption is the process of encoding or scrambling data stored on laptops, servers, tablets, and other endpoints so that it is unreadable and unusable unless a user has the correct decryption key thereby protecting the firm's network from risks posed by the use of various devices and access points;
3. Enforce multi-factor authentication (MFA) which is a method whereby the system grants access only after presenting two or more pieces of evidence (or factors) such as a combination of password, token, One Time Password (OTP) etc;

4. Filter malicious domain URLs and perform domain name servers (DNS) sinkholing to thwart common phishing attacks and restrict access to sites that may violate corporate policies, including social networking and abusive content;
5. Staff of Dealing Member's (Staff) should change the default user names and passwords on home networking equipment, such as Wi-Fi routers by referring to the user manuals. Default user names and passwords may be available to the public hence easy to compromise;
6. Staff should avoid clicking on links in unsolicited electronic mails;
7. Staff should always visit official websites of relevant organizations for desired information to prevent them falling prey to impersonating websites;
8. Staff should always seek independent verification of electronic mails, texts or phone calls from unknown individuals, especially those claiming to be from the National Centre for Disease Control (NCDC), World Health Organization (WHO) or other agencies of Government;
9. Staff should avoid opening attachments in electronic mails that claim to have more information regarding the COVID-19 pandemic or related matters;
10. Clients' instructions received by electronic mail should be followed up with telephone calls for confirmation;
11. Incoming calls requesting password resets or reporting lost phones or office equipment should be scrutinised and treated with reasonable caution;
12. Check for and apply software updates and patches to the operating system, routers and applications on a timely basis. This may also be managed centrally by the Information Technology Departments;
13. Make use of updated versions of remote access/meeting applications, ensuring that links to teleconferences are provided directly to invitees and not made publicly available. Passwords, waiting rooms, "host only" screen sharing options should also be used. This is recommended to prevent session interruption. You may refer to the recent guidance on Virtual Meetings issued by The Exchange and available at www.nse.com.ng (http://www.nse.com.ng/dealing-memberssite/Notices/NSE%20GUIDANCE%20ON%20COMPANIES%20VIRTUAL%20MEETINGS.pdf;
14. Dealing Members should provide staff with continuous sensitisation/training on how to connect securely to the office environment or office applications from a remote location, potential scams and other attacks described above; and
15. Dealing Members should provide staff with critical IT support staff contact information (e.g. whom to contact with IT questions and issues, how to contact them, when to contact them and how to handle emergency situations).

B. Business Continuity

The Exchange's Minimum Operating Standard (MOS) and **Rule 4.1: Requirement for Commencement of Operations,** Rulebook of The Exchange, 2015 (Dealing Members' Rules) requires Dealing Members to have a Business Continuity Plan (BCP) with schedules for simulation tests, to ascertain the adequacy and reliability of the BCP at least twice a year or in the event of changes in technology or business process.

Given The Exchange's requirement for Dealing Members to have a BCP in place to address emergencies or business disruptions, The Exchange is providing further guidance on ways Dealing Members can manage the present pandemic and strengthen their organisational resilience:

1. Disclose to customers how the BCP addresses the possibility of the current business disruption and how the firm plans to respond;
2. Develop a mechanism to promptly place a notice on the firm's website in the event that registered representatives are unable to communicate with customers, indicating to affected customers whom they may contact concerning execution of trades, their accounts, and access to funds and securities and how to contact those person(s);
3. Update and maintain emergency contact information, including one contact who is a member of senior management and a registered principal of the firm, and a second contact who is a member of senior management with knowledge of the firm's business operations;
4. Review the sufficiency of the existing BCP, with particular attention to whether they are sufficiently flexible to address effects of the recent outbreak of COVID-19 which includes the use of remote working arrangements, travel or transportation limitations, staff absenteeism, and technology interruptions or slowdowns. This may be in form of crisis management and emergency response plan;
5. Compare the measures currently implemented in response to the COVID-19 pandemic against the measures provided in the existing BCP and modify the BCP accordingly;
6. Notify The Exchange on any issues being faced in activating its BCP, including any disruptions to business and whether those disruptions are resolved or ongoing; and
7. Refer to The Exchange's BCP response to COVID-19 to Dealing Members in the communication dated 25 March 2020: ***COVID-19 Remote Trading Access*** which includes information on remote trading via FIX Protocol and the Virtual Private Network (VPN).

C. Fraud Prevention

Dealing Members are also reminded of the importance of reviewing and aligning their internal supervisory systems in order to mitigate the risk of fraud which may arise from the current crisis. Dealing Members are required to ensure that their current operational practices comply with The Exchange's applicable Rules on Supervision and Internal Control. These include Rule 9.3: **Supervision and Controls,** Rule 9.6: **Control of Offices and Trading Terminals** and Rule 11.2: **Supervision of Customer Accounts**, Rulebook of The Exchange, 2015 (Dealing Members' Rules)

Particular attention should be given to potential financial crimes likely to be caused by:

- opportunistic fraudsters and criminals (e.g. social engineering and phishing that may prey upon clients' fears and uncertainties); and
- reduction in compliance monitoring and controls due to the crisis.

Some practical tips for mitigating fraud listed below:

Tips for Mitigating the Risk of Fraud

1. Review internal systems for potential gaps in supervision and fraud detection due to current social distancing, reduced staff, and remote working;
2. Practice good governance by ensuring that any deviations from normal operating standards due to the current extraordinary circumstances are consistent with existing governance mechanisms and regulation, e.g., obtaining Management's or the Board's authorization. Such deviations should be properly documented with appropriate justification provided, the duration of the deviation clearly articulated, and if possible, a specific plan made to address the deviation when circumstances change;
3. Maintain proper audit trails with the available technological solutions under the current working conditions (e.g., remote working), consistent with The Exchange's requirements;
4. Maintain customer privacy and information security when working remotely, ensuring that internal systems are adequately secured using virtual private networks, software patches, and multi-factor authentication, while educating employees on how to maintain customer privacy and information security;
5. Maintain critical functions. The outbreak has undoubtedly forced Dealing Members to make difficult decisions about how best to allocate resources. It is however still critical to maintain high-priority compliance functions, such as AML/CFT monitoring; and
6. Watch out for red flags such as false identity scams**,** trades that involve urgency, vague and unverifiable credentials etc.

Finally, Dealing Members are reminded to ensure proper record keeping during this period as The Exchange will continue its monitoring and off-site examination activities**.**

For further clarification on the above, contact the Broker Dealer Regulation Department via nsebdr@nse.com.ng

Please be guided accordingly.

Olufemi Shobanjo
Head, Broker Dealer Regulation