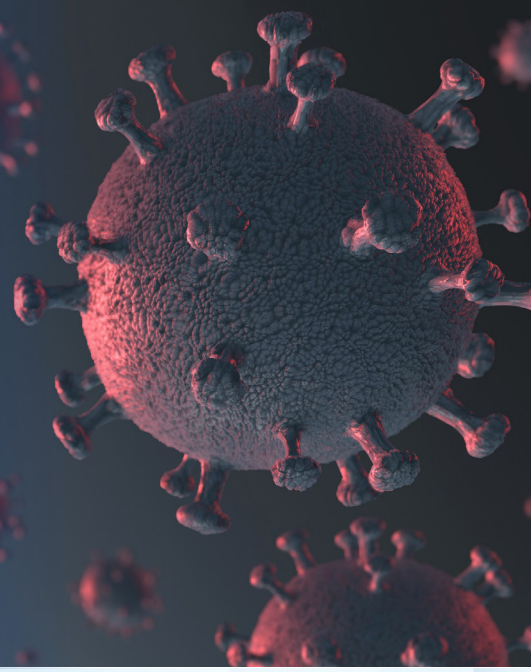
KPMG

Tackling Fraud Opportunities Arising from Working Remotely



Forensic Services

KPMG in Nigeria

April 2020

The COVID-19 pandemic has altered everything around us; from the way we interact to the way we work and communicate. Corporate entities and people are not just concerned but are working frantically to ensure safety and wellness of their employees, their loved ones, and at the same time, ensuring business continuity. This has resulted in the increased adoption of remote working.

Remote working of this particular nature, is an uncharted territory for many organisations and their employees. Fraudsters can consequently leverage and exploit certain opportunities and loopholes created with the increased uncertainty induced by the COVID – 19 pandemic.

The immediate concern regarding the current situation is that traditional fraud controls are being challenged, with more focus being shifted to cyberfraud.

Corporate entities should therefore pay more attention to the following, among others:

1. Increased reliance on virtual meeting platforms
2. Increase in use of e-signature
3. Use of personal devices and email accounts
4. Relaxed segregation of duties and controls
5. Possible increase in records falsification

Increased reliance on virtual meeting platforms

- Remote working has led to an increase in the use of virtual meeting platforms. These platforms may contain vulnerabilities that can be exploited by fraudsters. For example, it was recently alleged that a popular online meeting platform possesses a vulnerability that allows attackers steal windows login credentials, also "Zoombombing" damaged the integrity of the online meeting platform Zoom forcing them to make changes to their meeting structure.

Increase in use of e-signatures

- Contracts, invoices and sensitive documents that are usually printed and physically signed now have to be processed electronically with e-signatures and electronic letter heads. This may result in some fraud risks for organisations; such risks include:
  - easy and unauthorized reproduction of the organisation's letterheads and relevant e-signatures.
  - reduced ability to authenticate documents.

Use of personal devices and email accounts

- Company-issued devices tend to be equipped with relevant security solutions. However, in times like this, the number of employees connecting to their organisation's network via their personal devices will significantly increase. This consequently escalates the organisation's cyber-attack risks and loss of sensitive business and personal data, regardless of whether the personal devices have existing malware or not.
- Employees personal email accounts may have been ***phished*** or used to subscribe to certain sites, which may contain serious malware and other vulnerabilities. Using such accounts for business transactions can inadvertently expose the organisation.

Relaxed segregation of duties and controls

- The current situation is not business as usual and fraudsters may want to exploit this to their advantage by creating perceived emergency situations that may result in relaxed controls or disregard for existing segregation of duties.

Possible increase in records falsification

- Due to the restricted movements, employees and third-parties in remote locations may take advantage of this to falsify records such as:
  - Billing hours
  - Stock delivered/Service provided
  - Expense reports

How do you protect yourself

To address concerns highlighted in this publication, we should consider the following:

Virtual meeting platforms

- Utilise secure meeting platforms.
- Avoid reusing old meeting links as this increases the risk that an uninvited participant may attend the meeting. Generate a different link for every new meeting. Notwithstanding, always confirm that there are no alien participants attending the meeting.
- Minimise sharing sensitive information in the virtual meetings, as you can still use your secure email platform, for sharing sensitive information.

e-Signature and other electronic documents

- Ensure that electronic documents are adequately protected.
- Personally make use of your e-signature. Where not practicable, provide authorization for its use by another individual (documented in an email).
- Confirm invoices and sensitive information received from third-parties against previous communication with the third-parties before they are treated.
- Independently confirm any sudden change of the third-parties bank account details or email addresses, before using them.

Personal devices and email accounts

- Discourage use of personal email address for official transactions by not responding to such personal accounts. Where this is impossible, encrypt the information that is being transmitted via such personal email accounts, and communicate the password via another medium such as text or instant messaging.
- Always carefully check email addresses before responding.
- Increase employee awareness especially on how to avoid falling victim to phishing scams, during these period.

Other considerations include following:

- Ensure that hotline and whistleblowing channels are active and operational.
- Immediately report actual or suspected security events or suspicious activity to the appropriate functions.
- Update the rules and configuration on fraud management systems, taking cognizance of the new and emerging fraud risk landscape.
- Blacklist all non-essential applications in your network to reduce any possible security breach.
- Scale up computing capacity of applicable systems to process more volume given that there are more online transactions at this time.
- Leverage data analytics and other compensating controls to identify unusual spike in transactions.
- Limit employees connections to the organisation's network and resources through secure connections only, e.g. use of VPN.
- Continuously monitor remote access.
- Clearly define your protocols for emergency procurement and communicate to all relevant parties. This will include what will qualify for consideration, how and who will approve the procurement.
- Where practicable, limit procurement to existing and trusted suppliers.
- More importantly, continue to raise awareness among employees and other stakeholders.

For further questions or additional advice, please contact us.

Saheed Olawuyi
Partner & Head
Forensic Services
KPMG in Nigeria
E: saheed.olawuyi@ng.kpmg.com

Oluwaseun Odeku
Associate Director
Forensic Services
KPMG in Nigeria
E: oluwaseun.odeku@ng.kpmg.com

John Anyanwu
Partner
Technology Advisory
KPMG in Nigeria
E: john.anyanwu@ng.kpmg.com

Olutomilayo Ogunwole
Senior Manager
Forensic Technology Services
KPMG in Nigeria
E: Olutomilayo.Ogunwole@ng.kpmg.com

home.kpmg/ng
home.kpmg/socialmedia