



भारत प्रतिभूति मुद्रण तथा मुद्रा निर्माण निगम लिमिटेड

Security Printing and Minting Corporation of India Limited

मिनीरत्न श्रेणी-I, सीपीएसई
(भारत सरकार के पूर्ण स्वामित्वाधीन)

Miniratna Category-I, CPSE
(Wholly owned by Government of India)



भा.प्र.मु.मु.नि.नि.लि./सतर्कता/76/17/4 2 35
SPMCIL/VIG/76/17/

दिनांक 31 .01.2022
Date 31 .01.2022

परिपत्र संख्या 03/22/Circular No. 03/22

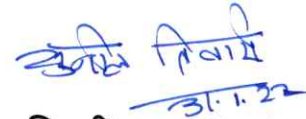
विषय/Sub:- सतर्क भारत: संरचनाओं और प्रक्रियाओं में प्रौद्योगिकी का लाभ उठाने के संदर्भ में/Vigilant India: Leveraging technology in structure and processes.

सीवीसी-सीबीआई के संयुक्त सम्मेलन में पैनल चर्चा के दौरान सतर्क भारत: संरचनाओं और प्रक्रियाओं में प्रौद्योगिकी का लाभ उठाने के विषय संदर्भ में श्री संदीप बलदावा सीनियर पार्टनर, फॉरेंसिक एंड इंटीग्रिटी सर्विसेज, ई एंड वाई इंडिया द्वारा "एक प्रवर्तक के रूप में प्रौद्योगिकी और सतर्कता पेशेवरों की भूमिका" पर दी गयी प्रस्तुतिकरण को जानकारी हेतु संलग्न पाये ।

A copy of presentation given by Shri Sandeep Baldava, Senior Partner, Forensic and Integrity Services, E&Y India on the subject: "Technology as an enabler and Way Ahead - Role of vigilance professionals" made during the panel discussion at joint conference of CVC and CBI at Kevadia on 20.10.2021 on topic of "Vigilant India: Leveraging Technology in structures and processes", is enclosed for information.

2. इसे सक्षम प्राधिकारी ने अनुमोदन से जारी किया जाता है।
2. This issues with the approval of Competent Authority.

संलग्न: यथोपरि / Encl: As above.



(सुनील तिवारी)/(Sunil Tiwari)

उप मुख्य सतर्कता अधिकारी/Dy. CVO

-पेज 2 - पर जारी

भा.प्र.मु.मु.नि.नि.लि./सतर्कता/76/17/
SPMCIL/VIG/76/17/

दिनांक .01.2022
Date .01.2022

सेवा में,/To,

मुख्य महाप्रबंधक/The Chief General Managers,

टकसाल/मुद्रणालय/कागज़ कारखाना/Mints/Presses/Paper Mill,

भा.प्र.मु.मु.नि.नि.लि./SPMCIL.

प्रतिलिपि/CC:

क) अध्यक्ष तथा प्रबंध निदेशक कार्यालय//CMD office.

ख) निदेशक (मा.स.) के कार्यालय सचिव/ निदेशक (वित्त) कार्यालय/ निदेशक (तकनीकी) के कार्यपालक सचिव / मुख्य सतर्कता अधिकारी के कार्यालय सचिव/ ES to Director (HR)/ Director (Finance) Office/ ES to Director (Technical)/ ES to CVO.

ग) मुख्य महाप्रबंधक (मा.स./तकनीकी)/ महाप्रबंधक (वित्त)/ अपर महाप्रबंधक (सूचना एवं प्रौद्योगिकी) डाटा सेंटर नोएडा/ CGM (HR/Tech)/GM (Finance)/ AGM(IT), Data Centre Noida.

घ) राजभाषा विभाग/ Department of Official Language

ड) सभी सतर्कता अधिकारी/All Vigilance Officials.

च) सूचना पटल एवं वेबसाइट/Notice Board & Website.

Sandeep Baldava, ACA, CFE, CISA

Sandeep Baldava is a Chartered Accountant, a Certified Fraud Examiner & a Certified Information Systems Auditor by qualification with over 25 years of professional experience. He has been associated with several reputed organisations and bodies dealing with Business Ethics, Anti-corruption, Internal Audit, and conducted multiple training workshops on Forensic Accounting, Fraud Risk Management, etc. Co-Author of Book "Forensic Investigations and Fraud Reporting in India"



1. Salient Features of the Presentation

1.1 Technology as an enabler

- 1.1.1 Technology has enabled governments and businesses to **successfully deliver effective solutions** for their respective stakeholders, including some solutions that were implemented on a mass scale and positively impacted the lives of millions of citizens
- 1.1.2 The adoption of technology has **reduced corruption** by increasing transparency through digital interactions and minimizing the need for citizens or businesses to interact physically with officers (train tickets, IT returns, etc)
- 1.1.3 The use of technology has **helped in mitigating frauds** (GPS tracking, Geo Tagging)
- 1.1.4 Technology and digital tools are **helping investigators crack cases faster** (example investigation of insider trading, money laundering, conflict of interest, etc)
- 1.1.5 However, ineffective understanding or over dependency **on technology** without sufficient knowledge of underlying loopholes and limitations may **give a false sense of comfort** – leading to r fraudsters/corrupt individuals to exploit the loopholes for personal gains
- 1.1.6 **TecKnowledgey** – the knowledge of technology and underlying loopholes is important for vigilance professionals to mitigate the risk of frauds and corruption
- 1.1.7 It is key to learn from real life case studies and understand loopholes in the system and improve it. Some examples include:

1.1.7.1 Manipulation of eBids or online auctions- a third party was appointed to improve the e-bidding system in an organization and were given admin access which was not disabled. This allowed them to share the data with a prospective bidder.

1.1.7.2 Duplicate payments on Enterprise Resource Planning (ERP) systems- within ERP, duplicate invoices are possible, for example by use of special characters, or using same invoice over two different quarters. Maker checker controls become redundant when people (maker or checker) share passwords.

1.1.7.3 Manipulation of biometric attendance records- in the factory premises of an organization, it was found that four fingers' imprint were taken of each individual as there were chances of workers getting hand injury and one finger imprint may not work. In the backend, these four fingers' imprint were not connected with one ID but were connected with four different IDs. In another case, it was found that the resolution was modified to 90 percent, which means pretty much anyone can give attendance for anyone else.

1.1.7.4 Electronic weighbridge manipulation- it was found that the weight of inventory varied depending on the placement or positioning of the vehicle on the weighbridge (either on the right side, left side or centre of the machine).

1.1.7.5 Disintegrated systems – manual intervention- today, the reconciliation process is only aimed at reconciliation and not identification of gaps and anomalies. This can give rise to a scenario where if a transaction shows amount is paid to X but it actually goes to Y. During reconciliation, the amount matches, but there is no way to find this anomaly.

1.1.7.6 GPS device tracking frauds- e.g. the device is removed from vehicle and GPS only tracks the device providing an opportunity for manipulation by fraudsters.

1.1.7.7 Ease of operation vs strict controls- e.g. when a new system is implemented, there are teething problems. Modifications are made to the system and in the process, overall control may be reduced. For e.g., backdating is not allowed. Employees may face problems in the month

of March when there are thousands of invoices. So, the system is enabled to allow backdating for a limited period. Adequate monitoring control is needed so this feature is used for limited periods and not for a longer duration.

1.1.7.8 Digital lending fraud – Digital lending frauds are on the rise with fraudsters building their online profiles based on pre-defined criteria which makes them eligible for pre-approved digital loans

2. Way Ahead

2.1 Role of vigilance professionals

2.1.1 Create awareness for all stakeholders in the organization to be vigilant

2.1.2 Proactive review and identification of vulnerabilities in digital processes and business models

2.1.3 Collaborating with management to help remediate and address the vulnerabilities

2.1.3 Leveraging technology

2.1.4.1 Use of forensic data analytics tools to proactively identify fraud patterns

2.1.4.2 Use of Robotic Process Automation (RPA) in Compliance and Vigilance

Disclaimer: Views expressed are personal and do not represent the views of the employer / organization that the speaker is/was associated with.