<u>The Bill Gates of KDS</u>:

A study of the existing IT System for bill processing and HR Management in Kolkata Dock System.

****

Some of the preventive functions prescribed by CVC (in their latest Vigilance Manual) for the Vigilance Wing of an Organization state the following:

> *"To undertake study of existing procedures and practices prevailing in his Organisation with a view to identify those procedures or practices which provide a scope for corruption and require modification; to identify the areas in his Organisation which are prone to corruption and to ensure that Officers of proven integrity only are posted in those areas; to ensure that well-defined internal processes as well as corresponding controls with clear responsibilities, for different kind of activities, are set out;"* [Chapter–II, Para 2.13 of Vigilance Manual 2017]

In pursuance of the above objective and consequent to a recent Vigilance Investigation into alleged electronic manipulation of salary & allowance by an officer of KoPT, a study was undertaken on the existing IT modules that deal with bill processing and HR Management functions of Kolkata Dock System. The study revealed vulnerabilities of such fundamental nature that it defies imagination as to how they could have remained undetected for years in modules that deal with Crores of rupees of financial disbursements to thousands of employees and record their critical career progression data. Following the investigation a series of systemic improvements was suggested by Vigilance Department which was approved by Chairman for immediate implementation.

<u>Case – I</u> : <u>Fraud in passing Medical Bills in the Pre-Computer Era</u>

In June 2017, an alert Finance Officer of Fringe Benefit (Medical) Section, attached to the Centenary Hospital of Kolkata Port Trust, accidentally detected a false claim for Medical reimbursement submitted by another senior Finance Officer. It is this Section which processes the Medical reimbursement claims of employees of KDS, after verifying relevant documents like Doctor's prescription, medicine purchase invoices, etc. A preliminary probe by Finance Department, prima facie, found the said Officer's Medical claim to be based on forged/fabricated Doctor's Prescription, had the said Officer suspended and referred the case to Vigilance for detailed investigation. The case appeared peculiar because only a couple of years ago, the said Officer himself headed the FB (Medical) Section and functioned as "Medical Bill Passing Officer" of the other employees of KDS. A question, therefore, arose whether the very authority, who was passing the bill of all employees, would do such manipulation in his own case?

Investigation found that such irregularities were not restricted to 2017 alone and had been going on for years. The nature of fraud was not only limited to production of forged Doctor's prescription, but a spectrum of similar irregularities. One of the detected irregularities deserve special attention from systemic point of view. It is concerning manipulation of a document called "Advice Summary". This "Summary", in pre-Computerization days, contained a list of names of employees and amount of Medical reimbursement passed against them, after due verification of claim papers submitted to FB(Medical) Section. It used to be prepared in 2 (two) copies. While 1 (one) copy used to be retained in the FB (Section), along with the claim papers, the other copy used to be sent to Pre-audit Section of HQ Finance, for inclusion in the monthly salary. For several months, the said Officer simply used to enter an amount, by hand, in the Pre-audit copy of "Advice Summary" for that month. Since the certified "Advice Summary" was supposed to come to Pre-Audit Section after due verification of all relevant documents submitted by the concerned employees, the Pre-audit Section used to incorporate the same in that month's salary. By this simple method, the suspected Officer could get Medical allowances, without submitting any claim related papers. A comparison between the copies kept in Pre-audit and FB(Medical) clearly established this easy manipulation that had gone undetected month after month, which was seemed to have been further helped by absence any kind of Post-audit of salary and allowances disbursed to employees.

<u>Case – II</u> : <u>The largest billing fraud by an individual employee</u>

Way back in 2006, a stunning Medical fraud of similar nature was noticed in Haldia Dock Complex (HDC) for a very large amount, nearly Rs. 42 Lakh. This was perpetrated by a single employee, who submitted a series of false Medical claims, immediately after retirement, for medicines prescribed by Tata Cancer Memorial Hospital, Mumbai and purchased from outside shops.**The "present value" of the defrauded amount would easily surpass the total drug – reimbursement expenditure for all employees in KDS in 2016-17, which happens be only Rs. 0.74 Crore.** The case came to light when accidentally, 1 (one) bill was put up to a Finance Officer, who was different from the chain of Officers who used to pass the earlier bills. The case, investigated by both Vigilance and CBI, resulted in Disciplinary Action against 7 (seven) Officials of HDC's Finance Wing. Following this, the process of Medical bill passing in HDC underwent total overhaul. It is, indeed, surprising that such a high profile case and the changes it brought about in HDC did not trigger any systemic change in the same process at KDS, even though both units are under the common administration of KoPT.

And now the case that triggered the above study.

<u>Case – III</u> : <u>Salary/Allowance Bill Processing Module with gates left ajar!</u>

In 2017, the Port Administration came across a case of attempted Electronic manipulation, by an Officer, to inflate his monthly salary, by making fictitious entries of allowances into the Computer system. What made the case ironical is that the same Officer was in charge of scrutinizing and passing salary bills of all employees of Kolkata

Dock System (KDS) and enjoyed sweeping access-rights to the relevant Computer modules. After a preliminary Departmental probe, the Port Administration suspended the Officer and handed over the case to Vigilance for a detailed investigation.
What initially seemed to Vigilance like a stray case of individual indiscretion, soon widened as more and more irregularities started cropping up. It was found that the Officer in question had made many such fictitious allowance entries into the Computer system in the past – almost at will – to defraud Port Trust for his pecuniary gain. As the investigation progressed further, it revealed a Computer system riddled with such basic deficiencies and faultiness that not just the aforesaid Officer, but anyone having access to these Modules, could have altered anything relating to salary, allowance or even service particulars, without leaving any meaningful Electronic footprint!

Indiscriminate sharing of User ID & Passwords that had powerful data rights in a system, through which Crores of Rupees were being disbursed, seemed to be the order of the day. Passwords of employees long transferred out of the Section still floated around, as no deactivation instruction had been issued to EDP, thereby leaving the system wide open to easy external manipulation. Ghost Passwords created in the system, on request of Finance Department, appeared to have remained inexplicably unused. Such a compromised system was further weakened by an "**Audit Trail Programme**" that had limited capability and did not preserve the "Original Data" once it got overwritten. Any system, so vulnerable and lacking basic internal controls, would naturally be a tempting target for any malicious user. While the manipulation by the Officer in question could be detected, given such a compromised system, a disturbing question emerges - *whether anyone else had made similar manipulation in the past and if so, how much Financial injury could have been sustained by KoPT in the years since these Modules came into existence?* That such frauds went on to happen, even after the billing process got Computerized, with Salary Module and associated Sub-modules for entering various Fringe Benefit allowances, goes on to support the age old proverb "***the more the things change, the more they remain same.***"

As the probe into serial Electronic manipulations made by the said Officer was drawing to a close, fresh complaint arrived with a startling allegation, i.e., that the very induction of the said Officer into KoPT service, through the died-in-harness route, as an LD Clerk, had been an act of identity-fraud perpetrated by him. When documents relating to his recruitment from his Personal File were called for, Finance Department informed that no such Personal File existed for him and so, no document – not even his appointment letter - could be produced to Vigilance (*It was later reported to Vigilance that no Personal File existed for almost all employees of Finance Department, numbering more than a hundred*).

Just when the investigation on the issue of fraudulent entry was about to hit a dead-end, information arrived that the very same allegation had been investigated by Vigilance Department years ago. A thorough search in Vigilance archives and a fortuitous retrieval of a 35-year old file revealed that indeed, these allegations had been investigated by Vigilance Department almost immediately after the Officer joined service in 1980. Vigilance had proved the fraud and the same had also been upheld in a Disciplinary Proceeding instituted subsequently by Port Administration. **Despite such**

proven serious charges, the Officer had been let off with an inconsequential punishment, under very questionable circumstances.

The same state of affairs continued even after a second Vigilance investigation proved the act of fraud and impersonation by the Officer in 2005. At that time also, lack of Personal File for the concerned Officer in Finance Department had been noticed by the then Vigilance Wing, prompting them to issue system improvement, in this regard. As latest investigation shows, the situation, instead of improving, has actually worsened over the years, necessitating the present system improvement. As for the Officer concerned, escape from any deterrent punishment from 2 (two)Vigilance investigations and a Disciplinary Proceeding that had intended to remove him from service, did not convert him to a repentant or reformed servant of the Trustee. Rather, after getting promoted to Officer cadre in 2013, he felt bold enough to upgrade his manipulative skills to the field of Electronic forgery, until he was accidentally caught and suspended.

SUGGESTED SYSTEM IMPROVEMENTS

1.0 **Sweeping access-rights to unworthy users**: In the present system, many employees lower down at the data-processing chain have been allotted rights to alter/delete/insert even master level data. In a processing flow, the access-rights should be commensurate with the level of the user. Rights to insert/update/delete sensitive data cannot be allowed to lower-level users. The requirement of rights vis-à-vis role of an employee in a given module must be immediately undertaken by EDP, in consultation with Finance.

2.0 **Improper access-rights assigned to Pre-audit personnel to change Sub-module level data without proper authorization**: One of the basic features of any Software system, which handles Financially sensitive information, is that the data created by one user should not be altered/deleted by another user, without appropriate higher level authorization and/or confirmation by the original data creator. In the present system, users in the main Payroll Module have been given rights to insert/update/delete the allowance that are sent from various Sub-modules like LTC and Medical reimbursement. In the present Business Process, employees first send their original documents related to their LTC or Medical reimbursement claim to the LTC/Medical reimbursement desk of the respective Sections. The personnel manning such desks verify the original claim papers and then enter the amount admissible to the employee into their respective allowance Sub-module. Thus, while the original claim documents remain in this Section after verification, the admissible amount entered into the Sub-module is transmitted to the main Payroll Module operated by Pre-audit Section for eventual incorporation into salary for the month. However, the Pre-audit Users have been given edit/insert right to the Sub-module level, without needing any authorization from that Section who first created this data. As a result, such a higher level user can simply insert any amount of "Allowance" for anyone, without any papers related to his allowance claim having been submitted to the respective allowance Sections. In fact, investigation has revealed that since Passwords/User IDs were being shared among many users of Pre-audit Section, the Officer in question used other's Password to change Sub-module level data. Therefore, edit/insert right to Pre-audit Section for data created by downstream Sub-modules must be withdrawn, as there is no such need. If such correction is required in some exceptional situation, then a change request to the original data-creator must be sent and change is to be effected, only after confirmation by Sub-module users.

3.0 **Absence of multi-level confirmation for modifying/inserting sensitive Payroll/ESR Module Data**: A very common feature of any Software that processes sensitive/Financial data is that higher level user(s) is/are required to confirm a change made by a lower level user for data not created by him/her. This is a must for ESR Module. Otherwise, anyone having a Password with insert/edit rights (and presently even lower level users have such rights) can alter anyone's service data. This will be impossible to detect in cases where there is no Personal File available for the employee. Hence, this feature should be immediately introduced.

4.0 **Validation with Digitally signed order/document**: Right now, many key fields related to career progression data of an employee, in ESR Module, can be altered by some Users in the Pre-audit Section. Since the existing Audit-trail utility does not preserve the original data once it gets changed, assigning such rights to a ESR-Module-User, without "rock-solid-validation", can create huge vulnerability, where the service record of an employee can be permanently changed, without verifiability. Hence, necessary validation for insert/update/delete of key fields in ESR module should be allowed to be effected, only when appropriate authority uploads a Digitally signed authority document into a text/OLE field. For instance, if an employee's pay in ESR is to be changed, then a pdf file of the circular/administrative order, Digitally signed by an appropriate authority, must be uploaded into the relevant validation field. Such Digitally signed document pertaining to career progression mile stones and bio-data of the employee can be assigned unique Document ID and can be linked to/stored in a Digital document vault to be securely stored in the Server.

5.0 Indiscriminate sharing of User IDs and Passwords: Sharing of Password/User ID, in a casual and irresponsible manner, which leads to loss of confidentiality and security, should be strictly forbidden. A total lack of awareness among users, about importance and confidentiality of User ID and Password, has been noticed during investigation. For instance, even though the data manipulation fraud by the Officer, described in the case study, came to light in June 2017, even after lapse of 6 (six) months, some employees examined by Vigilance were completely unaware of the need to maintain proper confidentiality of User ID/Password.

6.0 Free-floating Passwords, without deactivation and **Ghost User IDs in circulation**: It was observed during the investigations that User IDs and Passwords are generated by the Pre-audit Section and they are not deactivated, even after the concerned employee has been transferred from the Section long back. In a statement given to Vigilance, an employee has stated that he has never used an User ID and Password, but the documents show that an User ID and Password was created in his name and it has not been deactivated, although he has been transferred from the Pre-audit Section long back. Hence, all old User IDs/Passwords created in the system for transferred/retired users must be withdrawn by EDP.

7.0 Inadequate Audit trail utility, lacking elementary security feature: The Audit-trail features of the present Payroll and ESR Software Module are highly inadequate as they do not preserve "complete history" of changes made to the Master Data. For instance, if someone makes changes to an existing data field, say the "Date of joining" in the ESR Module, it would preserve the "Altered date of joining" and not the "Original date of joining". Thus, in case of suspected manipulation, the original data will never be known. Similarly, the present Audit-trail feature does not capture the Machine ID/Node ID from which the "change" might have been made by a malicious user. Enhancement of the existing Audit-trail utility, to capture detailed "change-history", including the Node/Machine Number, is not at all difficult and is, in fact, a common feature in all modern RDBMS like Oracle. **Since Salary/ESR Modules also use Oracle and KoPT has a Software Maintenance Contract worth Rs. 1.31 Crore, which includes "Module revamping", finalized in 2016, it is not understood why such a deficient Audit-trail utility has been allowed to continue for such a long time.**

8.0 Immediate formulation of a proper IT Security Policy: There should be a definite IT Security Policy circulated by EDP for covering generation of new Passwords, a secure channel for their communication to the intended users, deactivation procedure, etc. A Security Audit of the Computer Modules should be made once in every 3 (three) to 4 (four) years, either by competent EDP Officers having adequate professional expertise or by hiring an outside expert, if the former is not possible.

Taking lessons from the above investigation and case study, HoDs were advised to examine whether any IT System in their Department was being used for sensitive processes and to find out whether flaws of above nature exist in the same.

9.0 **<u>Non-existence of Personal File for employees of Finance Department</u>**: It is unfortunate that the above aspect had been noticed by Vigilance 13 (thirteen) years ago and system improvement advice had been given to FA&CAO, when allegation about impersonation by the Officer described in the case study was being investigated for the second time. At that time, Finance Department had informed that they do not maintain Personal Files for their employees. After 13 (thirteen) years, the present investigation finds that not only for the particular Officer, but for almost all employees of Finance Department, the same is true. <u>A serious time-bound effort is, therefore, needed to be made by Port Administration in general and Finance Department in particular, to collect their employees' KYC (Appointment Letter, Date of Birth, Educational Qualification, Career Progression Records, Disciplinary Proceeding History, etc.) and build the corresponding Personal Files.</u>

10.0 **<u>No checks for FD Card</u>**: The Family Declaration Card for the Officer, described in the case study, included 11 (eleven) members as "Dependent" family members. In fact, although the Officer in question was supposed to have been inducted through the died-in-harness route, his father was included in the FD Card and no one noticed it. <u>In view of this, a detailed mechanism must be laid down by LA&IR Davison for verification at the time of introduction of "Dependent" member</u>.

11.0 **<u>Rotational transfer of employees in sensitive posts</u>**: One aspect that needs immediate attention by the Apex Management is non-implementation of rotational policy in its true spirit. The case of passing fraudulent Medical bills in KDS, detected in 2017, was possible as 2(two) involved Supervisors of FB(Medical) Section, who were supposed to conduct verification of bill-related documents of claimant employees, were posted in Financially sensitive positions for 14 (fourteen) years and 10 (ten) years at a stretch. The suspected Officer, whose manipulated bills were detected, remained in a single post for 7 (seven) long years and in the same Section for 9 (nine) years. Frauds of the above nature are possible when employees remain entrenched in the same post/Section for long durations. It is only when a new person gets posted that possibility of any entrenched-fraud-chain getting broken arises. Banks are known to implement such policy with missionary zeal. In fact, Reserve Bank had implemented a "Mandatory Leave" policy since 2015, wherein employees in sensitive posts are required to compulsorily avail leave for a few days, in a single spell, every year and a new employee is made to work in his/her place. The idea being when a new person takes the seat, then he is likely to raise question about any suspicious irregular process, if persisting there. In Port Trust, often infeasibility of rotational transfer in many posts are pointed out, citing lack of sufficient number of domain experts required for specialized jobs. However, the same is not always true, especially for Finance Department. For instance, the total manpower of KDS Finance Department is 152 in KDS, while the same is 56 for HDC. There is great asymmetry, when one compares these2 (two) units in terms of cargo handled and revenue earned [Cargo volume in 2016-17: KDS = 16.80 MT ; HDC = 34.14 MT ;; Revenue earned: KDS = Rs.674 Crores ; HDC = Rs. 1293 Crores]. While a direct correlation between manpower of a Department in KDS with that in HDC may not be fair, given their respective functional specialties, rotational transfer of employees manning sensitive posts of Financial importance, within and across these 2 (two)units, may not be altogether impossible.

****