(c) The summary of the Report of the Task Force on NIP was released by the Finance Minister on 31st December, 2019. Currently, the NIP includes over 6,800 infrastructure projects accounting for an investment of over ₹ 111 lakh crore to be implemented over the period FY 2020 to FY 2025 by the Center, States and the private sector.

(d) Infrastructure investment is crucial for faster, sustainable and inclusive economic growth. It is expected that the planned infrastructure investment of ₹ 111 lakh crore over the period FY 2020 to FY 2025 will help the Indian economy reach the GDP target of $5 trillion by FY 2025.

Hacking of NDMC employees' bank accounts

2594. SHRI SANJAY RAUT: Will the Minister of FINANCE be pleased to state:

(a) whether bank accounts of more than 200 employees of New Delhi Municipal Corporation (NDMC) were allegedly hacked and money siphoned off in the first week of February;

(b) if so, details thereof indicating the number of such bank frauds/siphoned off cases registered with several banks during the last two years and Government's reaction thereto; and

(c) the details of steps taken or proposed to be taken against such bank frauds and safety measures taken by Government to protect bank account holders?

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE (SHRI ANURAG SINGH THAKUR): (a) to (c) As informed by Reserve Bank of India (RBI), the number of all types of frauds reported in the category "Card/Internet-ATM and Debit cards/ Credit cards/Internet banking" reported since 2017-18 is as below:–

Year	Number of Frauds
2017-18	34,791
2018-19	52,304
2019-20 (till September, 2019)	30,965

The data of organization-wise bank accounts hacked and money siphoned off is not centrally maintained.

RBI has issued circulars/guidelines from time to time regarding measures to minimise cyber threats related to online transactions and digital payments which, *inter-alia,* include:–

(i) RBI vide its circular on 'Enhancing Security of Card Transactions' dated 15.01.2020, has *inter alia* issued following guidelines to banks, card payment networks and non-bank PPI issuers:–

- All the cards (physical/virtual) at the time of issue/re-issue are to be enabled for use only at contact based points of usage within India.
- Facility to switch on/off and set/modify transaction limits limits (within the overall card limit, if any, set by the issuer) for all types of transactions-domestic and international, at PoS/ATMs/online transactions/contactless transactions, etc. on 24x7 basis to be provided.
- Alerts/information/status, etc., through SMS/e-mail, as and when there is any change in status of the card to be provided.

(ii) To ensure all active cards by them are EMV Chip and Pin-based.

(iii) RBI's circular on 'Control measures for ATMs - Timelines for compliance' dated 21.6.2018 advises banks to implement various control measures within a time bound manner, including implementation of anti skimming, white listing solution, up-gradation of software and to closely monitor the compliance.

(iv) RBI's Master Circular on 'Frauds-Classification and Reporting', dated 1.7.2015, advises concerned banks to examine the fraud cases and report them to law enforcement agencies, examine staff accountability, complete proceedings against the erring staff expeditiously, take steps to recover the amount involved in the fraud, claim insurance wherever applicable and streamline the system as also the procedures so that frauds do not recur.

(v) As per RBI's circular on 'Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions' dated 6.7.2017, in case of unauthorised transactions occurring due to contributory fraud/negligence/ deficiency on the part of the bank and due to third party breach with customer

notifying such unauthorized transaction to the bank within three working days of receiving communication from the bank, he/she is entitled to zero liability. Further, on being notified by the customer, the bank has to credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any).

(vi) To provide customers with 24x7 access through multiple channels (at a minimum via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorised transactions that have taken place and/ or loss or theft of payment instrument, such as, card, etc.

Frauds through fake invoices in Delhi

2595. SHRI NEERAJ SHEKHAR: Will the Minister of FINANCE be pleased to state:

(a) whether Anti Evasion Wing of Central GST has detected a big fraud of ₹ 214 crore through fake invoices in Delhi recently;

(b) if so, the details thereof;

(c) the details of frauds through fake invoices detected during the last two years, State-wise and year-wise along with the amount involved; and

(d) the details of revenue collection under GST during the last 12 months, month-wise?

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE (SHRI ANURAG SINGH THAKUR): (a) and (b) Yes, Sir. The details of the subject case are as under:

Name of the Entity	Quantum of Fraud Detected (₹ Crores)	No. of Persons Arrested
M/s Haryana Excell Forging	214	1

(c) Sir, the details of GST frauds through fake invoices detected are as under: