भारत सरकार

वित्त मंत्रालय

वित्तीय सेवाएं विभाग

लोक सभा

अतारांकित प्रश्न संख्या 1195

जिसका उत्तर सोमवार, 28 जुलाई, 2025/6 श्रावण, 1947 (शक) को दिया गया

एटीएम चोरी/धोखाधड़ी की घटनाएं

1195. डॉ. बच्छाव शोभा दिनेश:

क्या वित्त मंत्री यह बताने की कृपा करेंगे किः

(क) क्या सरकार ने भारतीय रिजर्व बैंक की भारत में बैंकिंग की प्रवृत्ति एवं प्रगति संबंधी रिपोर्ट 2023-24 का संज्ञान लिया है, जिसके अनुसार अप्रैल-सितंबर के दौरान कुल धोखाधड़ी के 18,461 मामले सामने आए, जिनमें 21,367 करोड़ रुपए की राशि शामिल थी, जबकि पिछले वित्तीय वर्ष की तुलनात्मक अवधि में धोखाधड़ी के 14,480 मामले सामने आए थे, जिनमें 2,623 करोड़ रुपए की राशि शामिल थी;

(ख) क्या एटीएम चोरी की बढ़ती घटनाओं को रोकने के लिए सरकार द्वारा कोई उपचारात्मक उपाय किए गए हैं;

(ग) क्या सरकार ने एटीएम कार्ड स्क्रीमिंग धोखाधड़ी की बढ़ती प्रवृत्ति का संज्ञान लिया है जिसमें अपराधी एटीएम उपयोगकर्ताओं से क्रेडिट या डेबिट कार्ड की जानकारी चुराने के लिए एक उपकरण का उपयोग करते हैं;

(घ) यदि हां, तो क्या सरकार ने इस संबंध में कोई सुधारात्मक उपाय किए हैं और यदि हां, तो तत्संबंधी ब्यौरा क्या है; और

(ड.) क्या सरकार ने एटीएम स्क्रीमिंग को रोकने के लिए अतिरिक्त सुरक्षा उपाय लागू करने के लिए सभी बैंकों को अधिदेशित करते हुए कोई निदेश जारी किया है और यदि हां, तो तत्संबंधी ब्यौरा क्या है और यदि नहीं, तो इसके क्या कारण हैं?

उत्तर

वित्त मंत्रालय में राज्य मंत्री (श्री पंकज चौधरी)

(क): भारतीय रिज़र्व बैंक की भारत में बैंकिंग के रुझान और प्रगति के संबंध में वर्ष 2023-24 की रिपोर्ट के अनुसार रिपोर्टिंग की तिथि के आधार पर 1 लाख रुपए और उससे अधिक की राशि वाली धोखाधड़ियों के आधार पर अप्रैल-सितंबर (2023-24) में हुई 2,623 करोड़ रुपए के 14,480 मामलों की तुलना में अप्रैल – सितंबर (2024-25) के दौरान हुई धोखाधड़ी संबंधी मामलों की संख्या 18,461 है जिसमें 21,367 करोड़ रुपए की राशि अंतर्ग्रस्त हैं।

वर्ष 2024-25 की छमाही (अप्रैल-सितंबर) के दौरान धोखाधड़ियों में वृद्धि पुन: जांच करने और पिछले वित्तीय वर्षों के 9,997 करोड़ रुपए वाली धोखाधड़ी से संबंधित 59 नये मामले के कारण हैं, जिसे बैंकों द्वारा 27 मार्च 2023 के माननीय उच्चतम न्यायालय के निर्णय का अनुपालन न करने के कारण पहले वापस ले लिया गया था और उपर्युक्त निर्णय का अनुपालन सुनिश्चित करने के बाद चालू वित्तीय वर्ष के दौरान बैंकों द्वारा इसकी पुन जांच की गई है और नए सिरे से सूचित किया गया है।

आरबीआई के आंकड़ों के अनुसार, घटना की तारीख के आधार पर वित्तीय वर्ष 2023-24 की 1 लाख और रुपए उससे अधिक राशिवाले 4,893 करोड़ रुपए की धोखाधड़ी के 34,121 मामले पाए गए हैं, जो वित्तीय वर्ष 2024-25 में घटकर 1,037 करोड़ रुपए की राशिवाले 10,175 मामले हो गए। इस प्रकार, पिछले 2 वर्षों में हुई धोखाधड़ी में गिरावट की प्रवृत्ति देखी जा सकती है।

(ख): आरबीआई, दिनांक 21.6.2018 के "एटीएम के लिए नियंत्रण उपाय-अनुपालन के घटनाक्रम" पर परिपत्र के माध्यम से बैंकों को एटीएम की सुरक्षा मजबूत करने के लिए विभिन्न उपाय करने की सलाह दी। इन उपायों में, अन्य बातों के साथ-साथ, बीआईओएस पासवर्ड सक्षम करना, यूएसबी पोर्ट को अक्षम करना, ऑटो-रन सुविधा को अक्षम करना, ऑपरेटिंग सिस्टम और अन्य सॉफ्टवेयर के नवीनतम पैच लागू करना, टर्मिनल सुरक्षा समाधान, समय-आधारित प्रशासकीय पहुंच, एंटी-स्किमिंग और वाईटलिस्टिंग समाधान लागू करना, परिचालन प्रणाली के सहायक संस्करणों में एटीएम का उन्नयन करना आदि शामिल हैं।

भारतीय रिजर्व बैंक ने बैंकों को लूटपाट आदि की घटनाओं से निपटने और ऐसी घटनाओं से होनेवाले जोखिम की अवधारणाओं से निपटने के लिए अपनी शाखाओं और एटीएम में सुरक्षा व्यवस्थाओं की समीक्षा करने और उसे मज़बूत करने के लिए समय-समय पर सलाह दी है। इनमें सी सी टी वी द्वारा एटीएम स्थलों की कवरेज, निजी सुरक्षा गार्डों के परिचय-पत्रों का सत्यापन, एटीएम पर तैनात सुरक्षा कर्मियों का पर्याप्त प्रशिक्षण सुनिश्चित करना आदि शामिल हैं।

बैंकों को चोरी (एटीएम चोरी सहित) पर तिमाही विवरणी पर्यवेक्षण विभाग, भारतीय रिजर्व बैंक को प्रस्तुत करनी अपेक्षित है। इस प्रकार एकत्र किए गए आंकड़ों को आरबीआई के क्षेत्रीय कार्यालयों के साथ साझा किया जाता है, और राज्य स्तरीय सुरक्षा समिति (एसएलएससी) की बैठकों के दौरान संबंधित राज्य प्राधिकारियों के साथ इस मामले पर चर्चा की जाती है।

(ग): आरबीआई की वर्ष 2024-25 की वार्षिक रिपोर्ट के अनुसार, रिपोर्टिंग की तारीख के आधार पर डिजिटल भुगतान (कार्ड/इंटरनेट) की श्रेणी के अंतर्गत धोखाधड़ी, जिसमें 1 लाख रुपये और उससे अधिक की राशि शामिल हैं, वित्तीय वर्ष 2023-24 के 29,082 मामलों में 1,457 करोड़ रुपये की राशि शामिल थी, जो वित्तीय वर्ष 2024-25 में घटकर 520 करोड़ रुपये की राशि वाले 13,516 मामलों तक रह गई। इस प्रकार, पिछले 2 वर्षों में रिपोर्ट किए गए कार्ड/इंटरनेट धोखाधड़ी में गिरावट की प्रवृत्ति दिखाई देती है।

(घ) और (ङ): जोखिम शमन उपाय के रूप में, आरबीआई ने मैग्नेटिक स्ट्राईप कार्ड से ईएमवी चिप और पिन आधारित कार्ड में बदलने के संबंध में सभी विनियमित संस्थाओं (आरई) को दिशानिर्देश जारी किया है।

भारत में बैंकों और व्हाइट लेबल एटीएम परिचालकों को यह सुनिश्चित करने के लिए कहा गया था कि उनके द्वारा स्थापित / संचालित सभी मौजूदा एटीएम 30 सितंबर, 2017 तक ईएमवी चिप और पिन कार्ड के संसाधन में सक्षम हों। प्रारंभ से ही ईएमवी चिप और पिन प्रोसेसिंग के लिए सभी नए एटीएम आवश्यक रूप से चालू किए जाएंगे।

कार्ड लेनदेनों, ऑनलाइन लेन-देनों आदि की सुरक्षा बढ़ाने और एटीएम बैंकिंग धोखाधड़ियों को कम करने के लिए व्यापक कदम उठाए गए हैं जिनमें, *अन्य बातों के साथ-साथ,* निम्नलिखित शामिल हैं:-

- आरबीआई ने तृतीय पक्ष एटीएम स्विच एप्लीकेशन सर्विस प्रोवाइडर्स (एएसपी) के लिए साइबर सुरक्षा नियंत्रण पर दिनांक 31.12.2019 को दिशानिर्देश जारी किए हैं।
- आरबीआई ने दिनांक 18.2.2021 को डिजिटल भुगतान सुरक्षा नियंत्रण पर मास्टर निदेश जारी किया है। इस निदेश के अनुसार, बैंकों को ग्राहक डेटा और उनके द्वारा प्रदान किए गए डिजिटल उत्पाद/सेवाओं से जुड़ी प्रक्रियाओं की गोपनीयता और सत्यनिष्ठा की रक्षा करने के लिए आवश्यक नियंत्रण रखने की सलाह दी गई है।
- 19 मई 2022 के आरबीआई परिपत्र सीओ.डीपीएसएस.पीओएलसी.सं.एस-227/02-10-002/2022-23 के अनुसार सभी बैंक, एटीएम नेटवर्क और व्हाइट लेबल एटीएम परिचालकों (डब्ल्यूएलएओ) के अनुसार उनके एटीएम पर इंटरऑपरेबल कार्ड-लेस कैश विदड्रॉल (आईसीसीडब्ल्यू) का विकल्प प्रदान कर सकते हैं। नकद आहरण लेन-देन शुरू करने के लिए कार्ड की आवश्यकता न होने से स्किमिंग, कार्ड क्लोनिंग, उपकरण में छेड़छाड़ (डिवाइस टेम्पेरिंग) आदि जैसी धोखाधड़ी को रोकने में मदद मिलेगी।
- धोखाधड़ी के खिलाफ जागरूकता फैलाने के लिए बैंक एटीएम और शाखाओं में पोस्टर लगाना।
- अप्राधिकृत लेनदेन जो हुए हैं की रिपोर्ट करने के लिए और/या पेमेंट उपकरण, जैसे कार्ड आदि की हानि या चोरी की सूचना देने के लिए विभिन्न चैनलों (वेबसाइट, फोन बैंकिंग, एसएमएस, ई मेल, आईवीआर, टॉल फ्री हेल्पलाईन, होम ब्रांच को रिपोर्ट करना आदि) के माध्यम से 24x7 पहुंच प्रदान करना।

*****