Press Release

Date: Jan 14, 2026

Office of Brijmohan Agrawal, Member of Parliament, Raipur, Lok Sabha

GOVERNMENT INTENSIFIES CRACKDOWN ON 'DIGITAL ARREST' SYNDICATES AMID STAGGERING LOSSES TO SENIOR CITIZENS

- Greater Kailash Couple Duped of ₹14.85 Crore; MP Brijmohan Agrawal Advocates for Singapore-Style 'Money Lock' Features
- MP Agrawal to Consult Finance Minister and RBI Governor on Mandatory Security Latches for Large Transactions
- Supreme Court Vows to Act with 'Iron Hands' as Nationwide Losses Breach ₹3,000 Crore Mark

NEW DELHI | January 14, 2026 – In a comprehensive reply tabled in the Lok Sabha, the Government of India today reaffirmed its commitment to dismantling the sophisticated "Digital Arrest" networks that have siphoned off thousands of crores from citizens. The formal response follows a harrowing case in South Delhi's Greater Kailash (GK), where an elderly doctor couple was kept under "virtual custody" for over two weeks, resulting in a theft of **₹14.85 crore**.

The recent fraud involving the Taneja family in Greater Kailash has sent shockwaves through the capital. Criminals, impersonating TRAI and law enforcement officials, coerced the victims into 15 days of continuous video surveillance. The Minister's reply highlighted that these syndicates exploit "psychological isolation," with funds siphoned via RTGS into multiple "mule accounts" across seven states.

Spearheading the legislative push for victim protection, Member of Parliament **Brijmohan Agrawal** raised a critical intervention in the House. Emphasizing the need for structural banking reforms to protect the elderly, Agrawal stated:

> *"We must adopt global best practices, such as the **'Money Lock' feature introduced by the Monetary Authority of Singapore (MAS)**. This allows users to 'lock' a portion of their funds from digital transfers, requiring physical verification or a different channel to unlock. I will personally speak to the **Hon'ble Finance Minister and the RBI Governor** to explore making such time-lock features mandatory for high-value accounts."*

The government's reply also cited the **Supreme Court of India's** recent *suo motu* cognisance of the menace. A bench led by Justice Surya Kant described the nationwide losses as "shocking" and directed a unified probe. The Apex Court has explicitly warned that it will deal with these fraudsters with **"iron hands,"** stressing that the forgery of judicial orders to intimidate citizens strikes at the very foundation of the legal system.

The MHA requested all citizens to adopt the **"Stop, Think, Act"** protocol. He noted that the **Indian Cyber Crime Coordination Centre (I4C)** has already blocked over 60,000 fraudulent IDs. Citizens are urged to immediately report suspicious calls to the **1930 Helpline**.

प्रेस विज्ञप्ति

तारीख: 14 जनवरी, 2025

कार्यालय - बृजमोहन अग्रवाल, संसद सदस्य, रायपुर, लोकसभा

बुजुर्गों की जमा-पूंजी पर डाका डालने वाले 'डिजिटल अरेस्ट' सिंडिकेट्स पर सरकार ने कसी नकेल

- ग्रेटर कैलाश के बुजुर्ग दंपत्ति से ₹14.85 करोड़ की ठगी; सांसद बृजमोहन अग्रवाल ने सिंगापुर की तर्ज पर 'मनी लॉक' फीचर की वकालत की
- बड़े वित्तीय लेन-देन के लिए अनिवार्य 'सिक्योरिटी लैच' पर केंद्रीय वित्त मंत्री और आरबीआई गवर्नर से चर्चा करेंगे सांसद अग्रवाल
- देशव्यापी ₹3,000 करोड़ की ठगी पर सुप्रीम कोर्ट सख्त, अपराधियों से 'लोहे के हाथों' से निपटने का संकल्प

नई दिल्ली | 14 जनवरी, 2026 – लोकसभा में प्रस्तुत एक विस्तृत उत्तर में, भारत सरकार ने आज उन परिष्कृत 'डिजिटल अरेस्ट' नेटवर्कों को ध्वस्त करने की अपनी अटूट प्रतिबद्धता दोहराई, जिन्होंने देश के नागरिकों से हजारों करोड़ रुपये ठगे हैं। यह औपचारिक वक्तव्य दक्षिण दिल्ली के ग्रेटर कैलाश (GK) के एक हृदयविदारक मामले के बाद आया है, जहां एक बुजुर्ग डॉक्टर दंपत्ति को दो सप्ताह से अधिक समय तक 'वर्चुअल कस्टडी' में रखकर ₹14.85 करोड़ की बड़ी राशि की चपत लगाई गई।

ग्रेटर कैलाश प्रकरण और कार्यप्रणाली ग्रेटर कैलाश के तनेजा परिवार के साथ हुई इस हालिया धोखाधड़ी ने राजधानी को झकझोर कर रख दिया है। खुद को ट्राई (TRAI) और जांच एजेंसियों का अधिकारी बताकर अपराधियों ने पीड़ितों को 15 दिनों तक निरंतर वीडियो निगरानी (डिजिटल अरेस्ट) में रहने के लिए मजबूर किया। मंत्री के जवाब में इस बात पर प्रकाश डाला गया कि ये सिंडिकेट "मनोवैज्ञानिक अलगाव" का फायदा उठाते हैं और RTGS के माध्यम से सात राज्यों में फैले कई 'म्यूल अकाउंट्स' में धन हस्तांतरित कर देते हैं।

संस्थागत सुधार के लिए बृजमोहन अग्रवाल की पहल पीड़ितों की सुरक्षा के लिए विधायी प्रयासों का नेतृत्व करते हुए, सांसद **श्री बृजमोहन अग्रवाल** ने सदन में एक महत्वपूर्ण हस्तक्षेप किया। बुजुर्गों की गाढ़ी कमाई की सुरक्षा के लिए बैंकिंग ढांचे में आमूल-चूल बदलाव की आवश्यकता पर जोर देते हुए अग्रवाल ने कहा:

> *"हमें सिंगापुर के मौद्रिक प्राधिकरण (MAS) द्वारा शुरू किए गए **'मनी लॉक' (Money Lock)** फीचर जैसे वैश्विक मानकों को अपनाना चाहिए। यह फीचर खाताधारकों को अपने धन के एक हिस्से को डिजिटल हस्तांतरण से 'लॉक' करने की अनुमति देता है, जिसे केवल भौतिक सत्यापन के जरिए ही अनलॉक किया जा सकता है। मैं व्यक्तिगत रूप से **माननीय वित्त मंत्री और आरबीआई गवर्नर** से भेंट कर उच्च-मूल्य वाले खातों के लिए ऐसे 'टाइम-लॉक' फीचर्स को अनिवार्य बनाने का आग्रह करूंगा।"*

सुप्रीम कोर्ट का 'लौह प्रहार' सरकार के जवाब में इस खतरे पर सुप्रीम कोर्ट द्वारा हाल ही में लिए गए 'स्वतः संज्ञान' (suo motu) का भी उल्लेख किया गया। जस्टिस सूर्यकांत की अध्यक्षता वाली पीठ ने ₹3,000 करोड़ के देशव्यापी नुकसान को "चौंकाने वाला" बताया है। शीर्ष अदालत ने स्पष्ट चेतावनी दी है कि वह इन धोखेबाजों से **"लोहे के हाथों" (iron hands)** से निपटेगी। कोर्ट ने कहा कि नागरिकों को डराने के लिए फर्जी न्यायिक आदेशों का उपयोग करना हमारी कानूनी व्यवस्था की नींव पर प्रहार है।

सतर्कता का आह्वान गृह मंत्रालय ने सभी नागरिकों से **"रुकें, सोचें, कार्य करें" (Stop, Think, Act)** प्रोटोकॉल अपनाने का अनुरोध किया है। सरकार ने सूचित किया कि भारतीय साइबर अपराध समन्वय केंद्र (I4C) अब तक 60,000 से अधिक धोखाधड़ी वाली आईडी ब्लॉक कर चुका है। किसी भी संदिग्ध कॉल की सूचना तुरंत **1930 हेल्पलाइन** पर देने का आग्रह किया गया है।

ई फा.सं. सीएसएफटी-01/68/2024

पंकज चौधरी
PANKAJ CHAUDHARY

सत्यमेव जयते

वित्त राज्य मंत्री
भारत सरकार
MINISTER OF STATE FOR FINANCE
GOVERNMENT OF INDIA

09 JAN 2026

प्रिय श्री बृजमोहन जी,

मैं आपका ध्यान दिनांक 11.12.2025 को शून्य काल के दौरान आपके द्वारा उठाए गए मामले की ओर आकृष्ट कराना चाहता हूं, जिसमें आपने 'एआई-संचालित सुरक्षा तंत्र' के संबंध में उल्लेख किया है।

2. इस संबंध में, मैं आपको अवगत कराना चाहता हूं कि भारतीय रिजर्व बैंक (आरबीआई) के परामर्श से इस मामले की जांच कराई गई है। भारतीय रिजर्व बैंक (आरबीआई) ने सूचित किया है कि उन्होंने धोखाधड़ियों के खतरे से निपटने के लिए प्रौद्योगिकी का उपयोग करते हुए कई उपाय किए हैं। पारंपरिक विनियामकीय/चेतावनी संबंधी उपायों/पर्यवेक्षी कार्रवाइयों/ग्राहक जागरूकता पहलों के अलावा, डिजिटल धोखाधड़ी की चुनौती से निपटने के लिए उभरती हुई तकनीक का उपयोग करके नवोन्मेषी तकनीकी उपकरण विकसित किए जा रहे हैं।

3. भारतीय रिज़र्व बैंक की पूर्ण स्वामित्व वाली सहायक कंपनी रिज़र्व बैंक इनोवेशन हब (आरबीआईएच) द्वारा उन्नत मशीन लर्निंग-आधारित समाधान, म्यूलहंटर.एआई.,विकसित किया गया है। पारंपरिक नियम-आधारित प्रणालियों के विपरीत, यह समाधान इकोसिस्टम लेवल लर्निंग के आधार पर विकसित वास्तविक दुनिया के धोखाधड़ी पैटर्न से प्राप्त व्यवहारिक और लेन-देन संबंधी विशेषताओं के विविध सेट का लाभ उठाता है ताकि प्रत्येक बैंक खाते को एक कॉन्फिडेंस स्कोर (संभावना) प्रदान किया जा सके , जो उसके म्यूल होने की संभावना को दर्शाएगा। इसके अलावा, भारतीय रिजर्व बैंक अपनी नवाचार सुविधा पहल, विनियामकीय सैंडबॉक्स और एचएआरबीआईएनजीईआर के माध्यम से इस समस्या का समाधान करने के लिए नवाचार को बढ़ावा दे रहा है।

5. इसके अलावा, साइबर वित्तीय धोखाधड़ी और डिजिटल अरेस्ट घोटालों पर अंकुश लगाने के लिए आरबीआई द्वारा उठाए गए कदमों और दिशानिर्देशों का सार अनुबंध में दिया गया है।

सादर,

आपका,

(पंकज चौधरी)

श्री बृजमोहन अग्रवाल,
माननीय संसद सदस्य (लोक सभा)
21, बी.आर. मेहता लेन,
नई दिल्ली –110001

जारी किया
ISSUED

डिजिटल अरेस्ट सहित डिजिटल धोखाधड़ी के निपटान के लिए आरबीआई द्वारा निम्नलिखित उपाय किए गए हैं:

i. डिजिटल धोखाधड़ी के निपटान में सहायता के लिए आरबीआई द्वारा आरंभ किए गए प्रमुखविनियामक उपायों में केवाईसी पर मास्टर निर्देशन, धोखाधड़ी जोखिम प्रबंधन (2024), साइबर सुरक्षा अवसंरचना (2016) और डिजिटल भुगतान सुरक्षा नियंत्रण (2021) पर मुख्य दिशानिर्देश शामिल हैं।

ii. अनधिकृत इलेक्ट्रॉनिक्स लेनदेन में बैंकों के लिए साझा देयता की जांच करने हेतु सीमित देयता अवसंरचना पहले से ही मौजूद है।

iii. भारतीय रिजर्व बैंक द्वारा गोपनीय परामर्श जारी किया जाता है जो बैंकों को साइबर धोखाधड़ियों के लिए नियंत्रण को सुदृढ़ करने और कानून प्रवर्तन एजेंसियों के साथ समन्वय करने का निदेश देता है।

iv. जहां भी आवश्यक पाया जाता है, समयबद्ध अनुपालन निर्देश, प्रवर्तन कार्रवाई और 'व्यापार प्रतिबंध' के रूप में प्रत्यक्ष पर्यवेक्षी कार्रवाई लागू की जाती है।

v. केवाईसी/एएमएल जोखिम का आकलन करने के लिए निरीक्षण और मनी म्यूल पर विषयगत मूल्यांकन, उसके पश्चात पर्यवेक्षी पत्र सुधारात्मक कार्रवाइयों को लागू करने में मदद करते हैं।

vi. एआई/एमएल आधारित 'म्यूलहंटर' प्लेटफॉर्म और रिजर्व बैंक इनोवेशन हब (आरबीआईएच) द्वारा विकसित डिजिटल पेमेंट्स इंटेलिजेंस प्लेटफॉर्म (डीपीआईपी) वास्तविक समय में संदिग्ध लेनदेन निगरानी में मदद करते हैं।

vii. केंद्रीय भुगतान धोखाधड़ी सूचना रजिस्ट्री (सीपीएफआईआर) भुगतान धोखाधड़ी की घटनाओं की रिपोर्टिंग और विश्लेषण को केंद्रीकृत करती है।

viii. आरबीआई ने बैंकों को दो-कारक अधिप्रमाणन, लेनदेन, वेलोसिटी निगरानी, कार्ड क्रेडेंशियल्स के टोकनाइजेशन, यूरोपे, मास्टरकार्ड और वीजा (ईएमवी) चिप-एंड-पिन प्रमाणीकरण और ग्राहक सक्षम कार्ड नियंत्रण को लागू करने की आवश्यकता के द्वारा डिजिटल भुगतान सुरक्षा को सुदृढ़ किया है।

ix. स्किमिंग जोखिम को कम करने के लिए यूपीआई के माध्यम से एटीएम पर इंटरऑपरेबल कार्डलेस कैश निकासी को सक्षम किया गया।

x. आरबीआई ने बैंकों को विशेष "bank.in" और "fin.in" डोमेन का उपयोग करना भी अनिवार्य किया है और ट्राई ने फिशिंग पर अंकुश लगाने के लिए कॉलिंग श्रृंखला को मंजूरी दी है।

xi. क्रेडिट कार्ड टोकेनाइजेशन अवसंरचना के माध्यम से, वास्तविक कार्ड विवरण को एक वैकल्पिक कोड के साथ प्रतिस्थापित किया जाता है जिसे 'टोकन' के रूप में जाना जाता है, जो ग्राहक के कार्ड के लिए एक विशिष्ट पहचानकर्ता के रूप में कार्य करता है।

xii. आरबीआई साइबर धोखाधड़ी के प्रभावी शमन के लिए आई4सी, डीओटी, टीआरएआई, एफआईयू-आईएनडी और एलईएएस के साथ सहयोग करता है। बैंकों को एनसीआरपी पोर्टल के साथ एकीकृत करने की सलाह दी गई है, जबकि वित्तीय धोखाधड़ी जोखिम संकेतक (एफआरआई) और मोबाइल नंबर निरसन सूची (एमएनआरएल) जैसे दूरसंचार उपकरण वित्तीय लेनदेन में दूरसंचार संसाधनों के दुरुपयोग की रोकथाम में मदद करते हैं।

*****

श्री बृजमोहन अग्रवाल (रायपुर) : माननीय सभापति महोदय, मैं आपसे आग्रह करना चाहता हूं कि डिजिटल अरेस्ट के माध्यम से एक गम्भीर समस्या उत्पन्न हो गई है, जो खासकर बुजुर्गों की आर्थिक सुरक्षा को खत्म कर रहा है। इस समय हम डिजिटल अरेस्ट फ्रॉड में एक खतरनाक बढ़ोतरी देख रहे हैं। यह एक बहुत ही जटिल अपराध है, जहां अपराधी वीडियो कॉल के जरिये सीबीआई या पुलिस अधिकारियों का रूप धारण करते हैं। वे पीड़ितों को कई दिनों तक डिजिटल निगरानी में रखते हैं और झूठी गिरफ्तारी की धमकी देकर उन्हें मनोवैज्ञानिक रूप से मजबूर करके उनकी पूरी जिंदगी की जमापूंजी खत्म करवा देते हैं। हाल ही में एक घटना हुई, जिसमें एक पीड़ित ने अपनी पूरी जिंदगी की कमाई की लगभग 30 करोड़ रुपये की रकम खो दी। ये छोटी-मोटी चोरियां नहीं है। यह पूंजी एवं मानसिक स्वास्थ्य का बहुत बड़ा नुकसान है, जो हमारे डिजिटल बैंकिंग सिस्टम की नाक के नीचे होता है। इसका मुख्य मुद्दा ट्रांसफर की स्पीड है। अब दबाव में आकर पीड़ित कुछ ही मिनटों में अपनी जिंदगी की कमाई की 80 से 90 प्रतिशत राशि सेविंग में ट्रांसफर कर सकता है। बैंकिंग सिस्टम इसे एक सही ट्रांजैक्शन के तौर पर प्रोसेस करता है, इसमें बदलाव होना चाहिए।

माननीय सभापति : आप अपनी मांग रखिए।

श्री बृजमोहन अग्रवाल (रायपुर) : महोदय, सिंगापुर के बैंक अब ज्यादा जोखिम वाले बदलाव के लिए मनी लॉक फीचर, कूलिंग ऑफ पीरियड का इस्तेमाल करते हैं। उदाहरण के तौर पर अगर कोई ट्रांजैक्शन किसी एकाउंट के बैलेंस के 50 प्रतिशत से ज्यादा रकम ट्रांसफर करने की कोशिश करता है, तो फंड को 12 से 24 घंटे के कूलिंग ऑफ पीरियड के लिए एक स्थायी एस्क्रो में भेज दिया जाता है। इसी से प्रेरणा लेकर मैं वित्त मंत्री जी से अनुरोध करता है कि नागरिकों के जीवन भर की बचत को बचाने के लिए सेफ्टी होल्ड फीचर या एस्क्रो मैकेनिज्म के लिए एआई के रिवेन गाइडलाइंस को जल्द से जल्द जारी करें।