

ફેક અને મ્યુલ એકાઉન્ટ

1) ફેક અને મ્યુલ એકાઉન્ટ : બેન્કિંગ અને સાયબર સુરક્ષા માટે વધતો ખતરો

આધુનિક ડિજિટલ યુગમાં બેન્કિંગ ક્ષેત્રે ટેકનોલોજીના વ્યાપક ઉપયોગને કારણે ગ્રાહકોને ઝડપી અને સરળ સેવાઓ ઉપલબ્ધ થઈ છે. પરંતુ બીજી તરફ સાયબર ગુનાઓ, આર્થિક છેતરપિંડી અને મની લોન્ડરિંગ જેવી પ્રવૃત્તિઓમાં પણ નોંધપાત્ર વધારો થયો છે. આવા ગુનાઓમાં “ફેક એકાઉન્ટ” અને “મ્યુલ એકાઉન્ટ”નો વ્યાપક ઉપયોગ થતો જોવા મળે છે. આ બંને પ્રકારના ખાતાઓ બેન્કિંગ વ્યવસ્થા, આર્થિક સુરક્ષા અને રાષ્ટ્રીય હિત માટે ગંભીર જોખમરૂપ છે.

2) ફેક એકાઉન્ટ શું છે?

ફેક એકાઉન્ટ એટલે ખોટી, બનાવટી અથવા ચોરી કરેલી ઓળખનો ઉપયોગ કરીને ખોલવામાં આવેલ બેન્ક ખાતું. આવા ખાતાઓ ખોલવા માટે ગુનેગારો ઘણીવાર ખોટા દસ્તાવેજો, ચોરાયેલા PAN/Aadhaar, ખોટા સરનામા અથવા નકલી મોબાઇલ નંબરનો ઉપયોગ કરે છે.

આજકાલ “Synthetic Identity”નો પણ વ્યાપક ઉપયોગ થાય છે, જેમાં સાચી અને ખોટી માહિતી ભેગી કરીને નવી ઓળખ ઉભી કરવામાં આવે છે. ઉદાહરણ તરીકે, એક વ્યક્તિનો PAN નંબર, બીજી વ્યક્તિનો ફોટો અને ત્રીજા વ્યક્તિનો મોબાઇલ નંબર મેળવી નવું ખાતું ખોલવામાં આવે છે.

3) મ્યુલ એકાઉન્ટ શું છે?

મ્યુલ એકાઉન્ટ એ એવું બેન્ક ખાતું છે જેનો ઉપયોગ ગેરકાયદેસર રીતે પ્રાપ્ત થયેલા નાણાંને એક જગ્યાથી બીજી જગ્યાએ ટ્રાન્સફર કરવા અથવા તેમના મૂળ સ્ત્રોતને છુપાવવા માટે કરવામાં આવે છે. મ્યુલ એકાઉન્ટ મોટેભાગે ભાડે લીધેલા ખાતાઓ છે. કોઈ સામાન્ય માણસ જેવાકે મજૂર, પ્લમ્બર, સફાઈ કામદાર વગેરેને તેમના ખાતાઓ વાપરવા માટે કમિશન આપવામાં આવે છે. તેમના ડેબિટ કાર્ડ, ચેક બુક, વગેરે ફોડ કરનાર પોતાની પાસે લઈ લે છે. અને ખાતા નો દુરુપયોગ કરે છે.

સાયબર ફોડ, ફિશિંગ, OTP છેતરપિંડી, રેન્સમવેર અથવા ઓનલાઇન સ્કેમ દ્વારા મેળવેલા નાણાં પહેલા આવા મ્યુલ એકાઉન્ટમાં જમા થાય છે અને ત્યારબાદ ઝડપથી અન્ય ખાતાઓ અથવા ક્રિપ્ટોકરન્સીમાં ટ્રાન્સફર કરવામાં આવે છે. આ પ્રક્રિયા દ્વારા ગુનેગારો નાણાંનો મૂળ સ્ત્રોત છુપાવવાનો પ્રયાસ કરે છે.

4) ફેક અને મ્યુલ એકાઉન્ટ કેવી રીતે કાર્ય કરે છે?

સામાન્ય રીતે ગુનેગારો નીચે મુજબની પદ્ધતિ અપનાવે છે:

1. ફિશિંગ અથવા સાયબર હુમલાથી વ્યક્તિગત માહિતી ચોરી કરવામાં આવે છે.
2. ચોરાયેલી માહિતીના આધારે નકલી KYC દસ્તાવેજો બનાવવામાં આવે છે.
3. આ દસ્તાવેજોનો ઉપયોગ કરીને ફેક બેન્ક ખાતું ખોલવામાં આવે છે.
4. સાયબર ફોડથી પ્રાપ્ત નાણાં મ્યુલ એકાઉન્ટમાં ટ્રાન્સફર થાય છે.
5. ત્યારબાદ નાણાંને વિવિધ ખાતાઓ, શેલ કંપનીઓ અથવા ક્રિપ્ટોકરન્સીમાં ફેરવવામાં આવે છે.

5) ફેક અને મ્યુલ એકાઉન્ટના મુખ્ય જોખમો

આવા ખાતાઓનો ઉપયોગ અનેક ગેરકાયદેસર પ્રવૃત્તિઓમાં થાય છે, જેમ કે:

- Money Laundering (મની લોન્ડરિંગ)
- Terror Financing (આતંકવાદી નાણાંકીય સહાય)
- Cyber Fraud (સાયબર છેતરપિંડી)
- Identity Theft (ઓળખ ચોરી)
- Tax Evasion (કર ચોરી)
- Loan Fraud (લોન છેતરપિંડી)
- Shell Company Fraud

આ ઉપરાંત બેન્કિંગ પ્રણાલી પ્રત્યે લોકોનો વિશ્વાસ પણ ઘટે છે.

6) ચેતવણીના મુખ્ય સંકેતો (Red Flags)

બેન્કો અને નાણાકીય સંસ્થાઓ માટે નીચેના સંકેતો મહત્વપૂર્ણ છે:

ચેતવણીનો સંકેત	સંભવિત જોખમ
એક જ મોબાઇલ નંબરથી અનેક ખાતા	ફેક એકાઉન્ટ
Dormant account અચાનક સક્રિય થવું	મ્યુલ પ્રવૃત્તિ
ઝડપી inward અને outward ટ્રાન્ઝેક્શન	મની લોન્ડરિંગ
KYC દસ્તાવેજોમાં ગેરમિલ	Forgery
અજાણી જગ્યાથી login	Account takeover

એક જ ડિવાઇસથી અનેક ખાતાઓનું સંચાલન Fraud Network

7) બચાવ માટે જરૂરી પગલાં

બેન્કો અને સંસ્થાઓ માટે

ફેક અને મ્યુલ એકાઉન્ટ સામે લડવા માટે બેન્કોએ મજબૂત નિયંત્રણો અમલમાં મૂકવા જોઈએ:

- Strong KYC અને Re-KYC પ્રક્રિયા
- Biometric Verification
- Liveness Detection
- AI આધારિત Fraud Monitoring

- Transaction Monitoring System
- Multi-Factor Authentication (MFA)
- Suspicious Transaction Reporting (STR)
- Employee Awareness Training
- Cybersecurity Monitoring

8) **RBI ની લેટેસ્ટ સૂચનાઓ અને નિયંત્રણો**

a) Strong KYC અને Re-KYC ફરજિયાત

બેન્કોને સૂચના આપવામાં આવી છે કે:

- Customer Due Diligence (CDD)
- Enhanced Due Diligence (EDD)
- Beneficial Ownership Verification

કઠોર રીતે અમલમાં મૂકવું.

ખાસ ધ્યાન:

- No PAN ખાતાઓ
- High-risk customers
- Multiple linked accounts
- Dormant accounts

પર ખાસ ધ્યાન રાખવાનું કહેવામાં આવ્યું છે.

b) Transaction Monitoring System (TMS)

બેન્કોએ Real-Time Monitoring કરવું જરૂરી છે. નવા ઓપન થયેલા ખાતાઓ અને ડોરમેન્ટ ખાતાઓ જો લાઈવ કરવામાં આવે તો બ્રાન્ચ મેનેજર ની તેવા ખાતાઓ મોનીટરીંગ કરવાની ફરજ છે અને તેવા ખાતામાં જો ગેરરીતિ (Red Flag પ્રવૃત્તિઓ) થાય તો તેમની જવાબદારી રહેશે.

નીચેના પ્રકારની પ્રવૃત્તિઓ Red Flag ગણાય:

- ઝડપથી inward-outward ટ્રાન્ઝેક્શન
- Round figure transactions
- Multiple small credits
- Dormant account activation
- High velocity fund movement
- Multiple beneficiary transfers

c) Suspicious Transaction Reporting (STR)

શંકાસ્પદ ટ્રાન્ઝેક્શનની માહિતી: Financial Intelligence Unit – India ને આપવી ફરજિયાત છે.

d) AI આધારિત “MuleHunter.AI”

RBI Innovation Hub દ્વારા “MuleHunter.AI” શરૂ કરવામાં આવ્યું છે.

આ સિસ્ટમ:

- i) AI/ML આધારિત છે **MuleHunter.AI** હાલમાં સક્રિય (active) છે અને ધીમે ધીમે ભારતની બેન્કિંગ સિસ્ટમમાં અમલમાં મૂકવામાં આવી રહી છે. આ સિસ્ટમ [Reserve Bank Innovation Hub \(RBIH\)](#) દ્વારા વિકસાવવામાં આવી છે.

તાજેતરના અહેવાલો મુજબ ઘણી મોટી Public Sector અને Private Sector Banks એ આ સિસ્ટમ અપનાવી લીધી છે. RBIH હજુ પણ બાકીની બેન્કોને જોડવા માટે કામ કરી રહી છે. લગભગ 28-30 બેન્કો platform સાથે integrated હોવાનું industry reports માં જણાવાયું છે. RTI આધારિત અહેવાલ મુજબ ઓછામાં ઓછી 23 બેન્કોએ MuleHunter.AI અમલમાં મૂકી છે.

- ii) મ્યુલ એકાઉન્ટના 19 પ્રકારના behavioral patterns શોધે છે

RBI અથવા RBI Innovation Hub દ્વારા હજુ સુધી આ “19 behavioral patterns” ની સત્તાવાર સંપૂર્ણ યાદી જાહેર કરવામાં આવી નથી. પરંતુ વિવિધ RBIH presentations, banking fraud analytics models, cyber fraud monitoring frameworks અને ઉપલબ્ધ industry references પરથી કેટલાક મુખ્ય patterns જાણી શકાય છે.

નીચે તે મહત્વપૂર્ણ behavioral indicators આપેલા છે જે MuleHunter.AI જેવા AI models સામાન્ય રીતે analyze કરે છે:

MuleHunter.AI દ્વારા ઓળખાતા સંભવિત 19 Behavioral Patterns

1. Rapid Inward-Outward Transactions

ખાતામાં પૈસા આવ્યા પછી તરત જ transfer થઈ જવું.

Example

₹50,000 credit → 5 મિનિટમાં debit.

2. Dormant Account Suddenly Active

લાંબા સમયથી inactive account અચાનક ભારે transaction કરવા લાગે.

3. High Velocity Transactions

ટૂંકા સમયમાં બહુ વધારે transactions.

4. Round Figure Transactions

₹10,000 / ₹50,000 / ₹1,00,000 જેવા fixed amounts.

5. Multiple Small Credits

ધણી નીચી credits જુદા જુદા accountsમાંથી આવવા.

6. Immediate Fund Layering

એક accountમાંથી બીજા અનેક accountsમાં ઝડપથી funds જવું.

7. Multiple Beneficiary Addition

ટૂંકા સમયમાં ઘણા beneficiaries ઉમેરવા.

8. Same Device Used for Multiple Accounts

એક જ mobile/device પરથી અનેક accounts ચલાવવાં.

9. Shared Mobile Numbers

ઘણા accountsમાં same mobile number.

10. Shared IP Address / Geo-location

એક જ location/IP પરથી multiple logins.

11. Frequent UPI Collections

UPI collect requests ઘણી frequent fund movement.

12. Unusual Login Timing

રાત્રે અથવા abnormal timing પર transactions.

13. Sudden Increase in Transaction Volume

અચાનક transaction amountમાં મોટો વધારો.

14. Frequent Cash Withdrawal After Credits

Credit આવ્યા પછી તરત cash withdrawal.

15. Account Used Only for Pass-Through

Balance maintain કર્યા વગર માત્ર transit account તરીકે ઉપયોગ.

16. Multiple Failed Authentication Attempts

Repeated OTP/password failures.

17. Emulator / Virtual Device Usage

Virtual Android devices અથવા emulatorsનો ઉપયોગ.

18. Frequent Change in Device or SIM

વારંવાર mobile/device/SIM બદલવા.

19. Suspicious Network Linkages

Accounts વચ્ચે hidden relationship:

- Same beneficiary
- Common introducer
- Same address
- Similar transaction chain

iii) **AI આ Patterns કેવી રીતે ઓળખે છે?**

MuleHunter.AI:

- Historical fraud data પરથી શીખે છે
- Normal customer behavior અને suspicious behavior compare કરે છે
- Hidden mule networks શોધે છે
- Risk score generate કરે છે

Example of AI Detection

ધારો કે:

- Dormant account સક્રિય થયું
- ₹20,000 ની 25 credits આવ્યા
- બધાં પૈસા 10 મિનિટમાં બીજા accountsમાં ગયા
- Same device પરથી 12 accounts operate થાય

તો AI તેને:

“High-Risk Mule Activity”
તરીકે flag કરી શકે.

- Suspicious accounts ઝડપથી ઓળખે છે

હવે બેન્કોને આ સિસ્ટમ અપનાવવા પ્રોત્સાહિત કરવામાં આવી રહ્યું છે.

e) **Dormant Accounts ઉપર વિશેષ દેખરેખ**

RBI એ બેન્કોને સૂચના આપી છે કે લાંબા સમયથી નિષ્ક્રિય ખાતાઓ અચાનક સક્રિય બને અને તેમાં ભારે ટ્રાન્ઝેક્શન થાય તો તરત Risk Review કરવો.

f) **Pre-Onboarding Checks ઝડક બનાવવી**

ખાતું ખોલતા પહેલાં:

- Device verification

- Mobile verification
- Geo-location checks
- Liveness detection
- Face match technology

ઉપયોગ કરવા પર ભાર મૂકાયો છે.

g) High-Risk Transaction Alerts

બેન્કોને AI આધારિત Alerts અને Risk Scoring System અમલમાં મૂકવાનું કહેવામાં આવ્યું છે.

ખાસ કરીને:

- Shell entities
- Fake merchant accounts
- Cryptocurrency linked transactions
- Cross-border remittances

ઉપર નજર રાખવાની સૂચના છે.

h) Real-Time Intelligence Sharing

RBI, I4C, FIU અને Law Enforcement Agencies વચ્ચે:

(I4C = Indian Cyber Crime Coordination Centre)

- Real-time data sharing
- Fraud intelligence sharing

વ્યવસ્થા મજબૂત કરવામાં આવી રહી છે.

I4C શા માટે બનાવવામાં આવ્યું?

ભારતમાં ઝડપથી વધી રહેલા:

- Cyber fraud
- Online scams
- Phishing
- Digital arrest fraud
- Banking fraud
- Social media crime
- Ransomware attacks

ને રોકવા માટે કેન્દ્ર સરકારે I4C સ્થાપિત કર્યું છે.

14C અને Mule Accounts

મ્યુલ એકાઉન્ટ સામે:

- Suspicious account tracking
- Fraud network mapping
- Real-time alerts
- Inter-bank intelligence sharing

કામ કરવામાં આવે છે.

“14C એ ભારત સરકારનું કેન્દ્રિય સાયબર ક્રાઇમ સંકલન મંચ છે, જે RBI, બેન્કો અને અન્ય એજન્સીઓ સાથે મળીને ડિજિટલ ફ્રોડ અને મ્યુલ એકાઉન્ટ સામે રિયલ-ટાઇમ ઇન્ટેલિજન્સ અને કાર્યવાહી સુનિશ્ચિત કરે છે.”

અને:

“ડિજિટલ બેન્કિંગના યુગમાં 14C જેવી સંકલિત વ્યવસ્થા સાયબર સુરક્ષા માટે અત્યંત મહત્વપૂર્ણ બની ગઈ છે.”

9. Employees માટે Accountability

બેન્ક સ્ટાફ દ્વારા:

- Improper account opening
- Weak KYC
- Fraud facilitation

થાય તો કડક કાર્યવાહી કરવાની સૂચના છે. તાજેતરમાં કેટલાક બેન્ક અધિકારીઓની ધરપકડ પણ થઈ હતી.

10. Customers માટે RBI ની સલાહ

ગ્રાહકોને સૂચના:

- પોતાનું ખાતું “ભાડે” ન આપવું
- OTP/PIN શેર ન કરવો
- અજાણ્યા ટ્રાન્ઝેક્શનથી સાવચેત રહેવું
- Commission માટે account operation ન કરવું કારણ કે મ્યુલ એકાઉન્ટમાં સામેલ વ્યક્તિ સામે પણ કાયદેસરની કાર્યવાહી થઈ શકે છે.
- OTP, PIN અથવા Password ક્યારેય શેર ન કરવો
- અજાણી લિંક્સ પર ક્લિક ન કરવું

- બેન્કિંગ માહિતી સુરક્ષિત રાખવી
- શંકાસ્પદ કોલ અથવા મેસેજથી સાવચેત રહેવું
- નિયમિત રીતે બેન્ક સ્ટેટમેન્ટ તપાસવું

10) સાયબર સુરક્ષા અને બેન્કિંગ વ્યવસ્થામાં મહત્વ

ફેક અને મ્યુલ એકાઉન્ટ માત્ર આર્થિક છેતરપિંડી પૂરતા મર્યાદિત નથી. તે રાષ્ટ્રીય આર્થિક સુરક્ષા, બેન્કિંગ સ્થિરતા અને સાયબર સુરક્ષા માટે પણ ગંભીર ખતરો ઉભો કરે છે. આજના ડિજિટલ યુગમાં મજબૂત KYC, સતત મોનિટરિંગ, ટેકનોલોજી આધારિત દેખરેખ અને કર્મચારીઓની જાગૃતિ અત્યંત જરૂરી બની ગઈ છે.

11) નિષ્કર્ષ

ફેક અને મ્યુલ એકાઉન્ટ બેન્કિંગ અને નાણાકીય ક્ષેત્ર માટે એક ગંભીર પડકાર છે. આવા ગુનાઓને રોકવા માટે માત્ર કાયદાકીય પાલન પૂરતું નથી, પરંતુ મજબૂત આંતરિક નિયંત્રણો, ટેકનોલોજી આધારિત સુરક્ષા વ્યવસ્થા અને ગ્રાહક જાગૃતિ પણ એટલી જ જરૂરી છે.

અંતમાં કહી શકાય કે:

“બેન્કિંગ ક્ષેત્રમાં વિશ્વાસ, પારદર્શિતા અને સુરક્ષા જાળવવા માટે ફેક અને મ્યુલ એકાઉન્ટ સામે સક્રિય અને સંકલિત પ્રયાસો અનિવાર્ય છે.”