



## उत्तर प्रदेश कोआपरेटिव बैंक लि०

मुख्यालय : 2, महात्मा गांधी मार्ग, लखनऊ-226 001

शाखा प्रबन्धक/मुख्य प्रबन्धक,  
उ०प्र० कोआपरेटिव बैंक लि०,  
समस्त शाखायें।

पी.बी.एक्स.

फैक्स

ग्राम

टेलेक्स

2623806,2623740

2624972,2611522

2214007

: 0522-2629284

: "प्रोबैंक"

: 0535-362 APEX IN

पत्रांक : के०वाई०सी०प्रकोष्ठ/2015-16/एफ-4/37/P.B.-

दिनांक : 04 जुलाई, 2015

276

गोपनीय

बैंक मुख्यालय के पत्रांक बैंकिंग/एफ-7/2007-08/सी-5, दिनांक 02.06.2007 के माध्यम से नकद लेन-देन रिपोर्ट (CTR) एवं संदिग्ध लेन-देन (STR) रिपोर्ट के प्रेषण के सम्बन्ध में निर्देश दिये गये हैं। उक्त परिपत्र के संलग्नक-1 पर संदिग्ध कार्यकलापों की निदर्शी सूची संलग्न है। पुनः बैंक मुख्यालय के पत्रांक:केवाईसी प्रकोष्ठ/2014-15/एफ-4/198, दिनांक 20.09.2014 के माध्यम से उत्कृष्ट संदिग्ध लेन-देन रिपोर्ट (STR) तैयार करने हेतु भारतीय रिजर्व बैंक का परिपत्र संख्या:RPCD.RCB.AML.No 12990/07.51.018/2013-14, दिनांक 26.05.2014 एवं एस.टी.आर. (STR) की पहचान एवं रिपोर्टिंग की प्रभावी प्रक्रिया से सम्बन्धित मार्गदर्शी नोट (Guidance Note) संलग्न कर अनुपालन हेतु आपको प्रेषित किया गया है। मार्गदर्शी नोट के मुख्य बिन्दु निम्नवत् हैं:-

### 1. जोखिम की पहचान एवं मूल्यांकन:-

#### (a) ग्राहक जोखिम (Customer Risk):-

उच्च/मध्यम श्रेणी ग्राहकों की सांकेतिक सूची एपेन्डिक्स E पर संलग्न की गयी है।

#### (b) उत्पाद एवं सेवा जोखिम (Product and Services Risk):-

उच्च एवं मध्यम जोखिम उत्पादों एवं सेवाओं से सम्बन्धित सांकेतिक सूची एपेन्डिक्स F पर संलग्न की गयी है।

#### (c) भौगोलिक जोखिम (Geography Risk):-

उच्च एवं मध्यम जोखिम श्रेणी Jurisdiction एवं Locations के आधार पर ग्राहक के लिए उच्चतर Due diligence रखा जाये। इसके लिए निम्नांकित बिन्दु विचारणीय हैं:-

1. व्यक्ति की नागरिकता का देश
2. व्यक्ति के निवास के पता का देश
3. विधिक संस्था के गठन का देश
4. मुख्य शेयरधारकों/लाभार्थी स्वामियों के निवास का देश
5. व्यवसाय के रजिस्ट्रेशन का देश
6. फण्ड के स्रोत का देश

7. व्यवसाय का देश

8. पत्राचार के पता का देश

9. ग्राहक के व्यवसाय के फैलाव के देश

विभिन्न देशों के साथ-साथ भारतवर्ष के अन्दर भौगोलिक स्थिति को भी धनशोधन (Money Laundering) एवं आतंकवादियों को वित्तपोषण (Terrorist Financing) के जोखिम के आधार पर वर्गीकरण किया जाना चाहिए।

## 2. संदिग्ध लेन-देन की पहचान हेतु Alerts :-

### (a) Alerts through AML Package :-

एएमएल पैकेज विभिन्न एवं स्पष्ट नियमों के आधार पर कई प्रकार के Alerts उत्पन्न करता है।

उच्च/मध्यम श्रेणी ग्राहकों की सांकेतिक सूची एपेन्डिक्स E पर संलग्न की गयी है।

### (b) Behavioural Alerts :-

इस प्रकार के विभिन्न एलर्ट Indicators की सांकेतिक सूची एपेन्डिक्स A पर संलग्न है।

### (c) Law Enforcement Agency द्वारा नोटिस/पत्र:-

किसी Law Enforcement Agency से नोटिस/पत्र प्राप्त होने की दशा में शाखा को अविलम्ब STR प्रेषित करना चाहिए। खाता बन्द होने की दशा में भी उसको रिपोर्ट किया जाये।

### (d) Adverse Media News :-

ग्राहकों का नाम समाचार में दिये गये संदिग्ध अथवा दोषी व्यक्तियों के साथ मिलान होने पर शाखा को अविलम्ब STR प्रेषित करना चाहिए। इसके साथ ही उनके खातों में लेन-देन का विश्लेषण भी किया जाना चाहिए।

### (e) CTR एवं NTR :-

शाखा द्वारा रिपोर्ट किये गये CTR एवं NTR में लेन-देन की समीक्षा गम्भीरतापूर्वक किया जाये। यदि ऐसे खातों में लेन-देन संदिग्ध पाया जाता है तो केवल CTR एवं NTR में रिपोर्ट करने मात्र से शाखा इन खातों को STR में रिपोर्ट करने के उत्तरदायित्व से बच नहीं सकेगी।

### (f) Red Flag Indicators :-

भारतीय बैंक संघ (IBA) द्वारा कई प्रकार के Red Flag Indicator सुझाये गये हैं जो बैंकों द्वारा लागू किया जाना आवश्यक है। इस प्रकार के Indicators की सूची एपेन्डिक्स B पर संलग्न है। इसमें से अधिकांश कम्प्यूटराइज्ड सिस्टम (Computerised system) द्वारा आच्छादित होते हैं। फिर भी कुछ Alerts को Computerised system द्वारा देखा नहीं जा सकता है और उनकी समीक्षा मैनुअल आधार पर होनी चाहिए।

(g) मल्टी लेवल मार्केटिंग फर्म के खातों की निगरानी :-

ऐसे खाते जिनमें जनता की भारी धनराशि जमा होती है और उनमें अत्यधिक संख्या में चेकबुक निर्गत की गयी है। खातों में निर्गत की गयी चेकबुकों में से अधिकांश अप्रयुक्त (Unused) है। ऐसे खातों की पहचान कर रिपोर्ट करना चाहिए।

(h) Beneficial owner :-

शाखाओं को खाते में लेन-देन के विश्लेषण के समय Beneficial owner की पहचान करनी चाहिए और मध्यवर्तियों द्वारा रखे गये खातों की सही प्रकृति को समझना चाहिए।

(i) Trade finance :-

समस्त प्रकार के इम्पोर्ट, एक्सपोर्ट एवं उच्च जोखिम देश को किये गये धन प्रेषण की समीक्षा करनी होगी।

(j) Overseas forex Trading:-

विदेशी एक्सचेंज में ऑनलाइन ट्रेडिंग करने वाले ग्राहक जो प्रारम्भ में भारतीय बैंक खाते से क्रेडिट कार्ड या इलेक्ट्रानिक चैनल से धन प्रेषण करते हैं या उसके बाद नकद धन वापसी प्राप्त करते हैं। ऐसे मामले को भी एसटीआर में रिपोर्ट करना चाहिए।

(k) Demat Accounts:-

NSDL एवं CDSL द्वारा मासिक आधार पर प्रेषित Alerts का विश्लेषण किया जाना चाहिए।

(l) Locker Operation:-

लॉकर से जुड़े खातों में अत्यधिक परिचालन का विश्लेषण करना चाहिए। जैसे कि नकद भुगतान के तुरन्त बाद लॉकर का परिचालन किया जाना अथवा लॉकर के परिचालन के तुरन्त बाद नकद जमा किया जाना।

3. संदिग्ध लेन-देन की पहचान के स्रोत :-

शाखाओं हेतु सांकेतिक Alert Indicators एपेन्डिक्स A पर संलग्न है। संदिग्ध लेन-देन की पहचान के स्रोतों का विवरण निम्नवत् है:-

(a) Customer verification(CV) :-

ग्राहक द्वारा जाली पहचान पत्र अथवा गलत पता प्रस्तुत करना।

(b) Law Enforcement Agency Query (LQ) :-

विधि प्रवर्तक एजेंसी या इन्टेलीजेन्स एजेंसी द्वारा खातों का संचालन रोकने, लेन-देन का विवरण भेजने हेतु पत्र/नोटिस प्राप्त होना।

(c) Media Report (MR) :-

मीडिया से ग्राहकों के विरुद्ध समाचार प्राप्त होना।



## (d) Employee Initiated (EI):-

किसी कर्मचारी द्वारा Alert दिया जाना। उदाहरण स्वरूप लेन-देन के सम्बन्ध में ग्राहक के पास कोई सूचना न होना, लेन-देन का प्रयास किया जाना ( Attempted Transactions ) इत्यादि।

## (e) Public Complaint (PC) :-

सामान्य जनता से खाते का प्रयोग फ़ाड के लिए किये जाने की शिकायत प्राप्त होना।

## (f) Business Associates (BA):-

अन्य संस्थाओं से सूचनायें प्राप्त होना।


## 4. Management of Alerts :-

शाखा द्वारा STR के रूप में प्रेषित करने के पूर्व विभिन्न स्रोतों से प्राप्त Alerts की पुनः समीक्षा किया जाना आवश्यक है। समीक्षा के दौरान निम्नांकित बिन्दु विचारणीय है:-

1. एलर्ट का स्रोत एवं चिन्हित Alerts Indicator
2. ग्राहक प्रोफाइल
3. जोखिम श्रेणी
4. लेन-देन का पैटर्न
5. प्राप्त की गयी अतिरिक्त सूचनायें

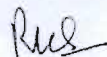
भारतीय रिजर्व बैंक द्वारा प्रेषित किये गये मार्गदर्शी नोट (Guidance Note) के साथ संलग्न एपेन्डिक्स A, B, C, D, E एवं F की छायाप्रतियाँ पुनः संलग्न कर इस निर्देश के साथ प्रेषित की जा रही हैं कि संदिग्ध लेन-देन की पहचान हेतु मार्गदर्शी नोट में दिये गये निर्देशों का कड़ाई से अनुपालन करना सुनिश्चित करें और कम्प्यूटर सिस्टम में AML Software की व्यवस्था होने तक मार्गदर्शी नोट में दिये गये अन्य बिन्दुओं के अनुसार संदिग्ध लेन-देन की पहचान हेतु लेन-देन की निगरानी एवं समीक्षा का कार्य मैनुअल आधार पर सर्तकता एवं गम्भीरतापूर्वक सम्पादित करना सुनिश्चित करें।

संलग्नक: यथोक्त।

  
( रवि कान्त सिंह )  
प्रबन्ध निदेशक

प्रतिलिपि: निम्नलिखित को सूचनार्थ प्रेषित:-

1. मुख्य महाप्रबन्धक, उ.प्र. कोआपरेटिव बैंक लि., मुख्यालय-लखनऊ।
2. समस्त महाप्रबन्धक/उपमहाप्रबन्धक/विभाग प्रभारी, उ.प्र. कोआपरेटिव बैंक लि., मुख्यालय-लखनऊ।
3. स्टाफ आफिसर-अध्यक्ष, उ.प्र. कोआपरेटिव बैंक लि., लखनऊ को अध्यक्ष महोदय के अवलोकनार्थ प्रस्तुत करने हेतु।

  
प्रबन्ध निदेशक

Appendix A

Indicative Alert Indicators for Branches

S. No.	Alert Indicator	Indicative Rule / Scenario
1	CV1.1 - Customer left without opening account	• Customer did not open account after being informed about KYC requirements
2	CV2.1 - Customer offered false or forged identification documents	• Customer gives false identification documents or documents that appears to be counterfeited, altered or inaccurate
3	CV2.2 - Identity documents are not verifiable	• Identity documents presented are not verifiable i.e. Foreign documents etc.
4	CV3.1 - Address found to be non existent	• Address provided by the customer is found to be non existent
5	CV3.2 - Address found to be wrong	• Customer not staying at address provided during account opening
6	CV4.1 - Difficult to identify beneficial owner	• Customer uses complex legal structures or where it is difficult to identify the beneficial owner
7	LQ1.1 - Customer is being investigated for criminal offences	• Customer has been the subject of inquiry from any law enforcement agency relating to criminal offences
8	LQ2.1 - Customer is being investigated for TF offences	• Customer has been the subject of inquiry from any law enforcement agency relating to TF or terrorist activities
9	MR1.1 - Adverse media report about criminal activities of customer	• Match of customer details with persons reported in local media / open source for criminal offences
10	MR2.1 - Adverse media report about TF or terrorist activities of customer	• Match of customer details with persons reported in local media / open source for terrorism or terrorist financing related activities
11	EI1.1 - Customer did not complete transaction	• Customer did not complete transaction after queries such source of funds etc.
12	EI2.1 - Customer is nervous	• Customer is hurried or nervous
13	EI2.2 - Customer is over cautious	• Customer over cautious in explaining genuineness of the transaction.

S. No.	Alert Indicator	Indicative Rule / Scenario
14	EI2.3 - Customer provides inconsistent information	<ul style="list-style-type: none"> <li>• Customer changes the information provided after more detailed information is requested.</li> <li>• Customer provides information that seems minimal, possibly false or inconsistent.</li> </ul>
15	EI3.1 - Customer acting on behalf of a third party	<ul style="list-style-type: none"> <li>• Customer has vague knowledge about amount of money involved in the transaction.</li> <li>• Customer taking instructions for conducting transactions</li> <li>• Customer is accompanied by unrelated individuals.</li> </ul>
16	EI3.2 - Multiple customers working as a group	<ul style="list-style-type: none"> <li>• Multiple customers arrive together but pretend to ignore each other</li> </ul>
17	EI4.1 - Customer avoiding nearer branches	<ul style="list-style-type: none"> <li>• Customer travels unexplained distances to conduct transactions</li> </ul>
18	EI4.2 - Customer offers different identifications on different occasions	<ul style="list-style-type: none"> <li>• Customer offers different identifications on different occasions with an apparent attempt to avoid linkage of multiple transactions.</li> </ul>
19	EI4.3 - Customer wants to avoid reporting	<ul style="list-style-type: none"> <li>• Customer makes inquiries or tries to convince staff to avoid reporting.</li> </ul>
20	EI4.4 - Customer could not explain source of funds	<ul style="list-style-type: none"> <li>• Customer could not explain source of funds satisfactorily</li> </ul>
21	EI5.1 - Transaction is unnecessarily complex	<ul style="list-style-type: none"> <li>• Transaction is unnecessarily complex for its stated purpose.</li> </ul>
22	EI5.2 - Transaction has no economic rationale	<ul style="list-style-type: none"> <li>• The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer.</li> </ul>
23	EI5.3 - Transaction inconsistent with business	<ul style="list-style-type: none"> <li>• Transaction involving movement of which is inconsistent with the customer's business</li> </ul>
24	EI6.1 - Unapproved inward remittance in NPO	<ul style="list-style-type: none"> <li>• Foreign remittance received by NPO not approved by FCRA</li> </ul>
25	PC1.1 - Complaint received from public	<ul style="list-style-type: none"> <li>• Complaint received from public for abuse of account for committing fraud etc.</li> </ul>
26	BA1.1 - Alert raised by agent	<ul style="list-style-type: none"> <li>• Alert raised by agents about suspicion</li> </ul>
27	BA1.2 - Alert raised by other institution	<ul style="list-style-type: none"> <li>• Alert raised by other institutions, subsidiaries or business associates including cross-border referral</li> </ul>



## Appendix B

### Red Flag Alerts:

S. No.	Alert Indicator	Indicative Rule / Scenario
1	WL1.1 - Match with UN list	<ul style="list-style-type: none"> <li>Match of customer details with individuals/ entities on various UNSCR Lists</li> </ul>
2	WL1.2 - Match with UAPA List	<ul style="list-style-type: none"> <li>Match of customer details with designated individuals/entities under UAPA</li> </ul>
3	WL1.3 - Match with other TF list	<ul style="list-style-type: none"> <li>Match of customer details with TF suspects on lists of Interpol, EU, OFAC, Commercial lists (World-Check, Factiva, LexisNexis, Dun &amp; Bradstreet etc.) and other sources</li> </ul>
4	WL2.1 - Match with other criminal list	<ul style="list-style-type: none"> <li>Match of customer details with criminals on lists of Interpol, EU, OFAC, Commercial lists (World-Check, Factiva, LexisNexis, Dun &amp; Bradstreet etc.) and other sources</li> </ul>
5	TM1.1 - High value cash deposits in a day	<ul style="list-style-type: none"> <li>Cash deposits greater than INR [X1] for individuals and greater than INR [X2] for non individuals in a day</li> <li>Top [N] cash deposits in a day</li> </ul>
6	TM1.2 - High value cash withdrawals in a day	<ul style="list-style-type: none"> <li>Cash withdrawals greater than INR [X1] for individuals and greater than INR [X2] for non individuals in a day</li> <li>Top [N] cash withdrawals in a day</li> </ul>
7	TM1.3 - High value non-cash deposits in a day	<ul style="list-style-type: none"> <li>Non-Cash deposits greater than INR [X1] for individuals and greater than INR [X2] for non individuals in a day</li> <li>Top [N] non-cash deposits in a day</li> </ul>
8	TM1.4 - High value non-cash withdrawals in a day	<ul style="list-style-type: none"> <li>Non-Cash withdrawals greater than INR [X1] for individuals and greater than INR [X2] for non individuals in a day</li> <li>Top [N] non-cash withdrawals in a day</li> </ul>
9	TM2.1 - High value cash deposits in a month	<ul style="list-style-type: none"> <li>Cash deposits greater than INR [X1] for individuals and greater than INR [X2] for non individuals in a month</li> <li>Top [N] cash deposits in a month</li> </ul>

S. No.	Alert Indicator	Indicative Rule / Scenario
10	TM2.2 - High value cash withdrawals in a month	<ul style="list-style-type: none"> <li>Cash withdrawals greater than INR [X1] for individuals and greater than INR [X2] for non individuals in a month</li> <li>Top [N] cash withdrawals in a month</li> </ul>
11	TM2.3 - High value non-cash deposits in a month	<ul style="list-style-type: none"> <li>Non-Cash deposits greater than INR [X1] for individuals and greater than INR [X2] for non individuals in a month</li> <li>Top [N] non-cash deposits in a month</li> </ul>
12	TM2.4 - High value non-cash withdrawals in a month	<ul style="list-style-type: none"> <li>Non-Cash withdrawals greater than INR [X1] for individuals and greater than INR [X2] for non individuals in a month</li> <li>Top [N] non-cash withdrawals in a month</li> </ul>
13	TM3.1 - Sudden high value transaction for the client	<ul style="list-style-type: none"> <li>Value of transaction is more than [Z] percent of the previous largest transaction for the client (or client profile)</li> </ul>
14	TM3.2 - Sudden increase in value of transactions in a month for the client	<ul style="list-style-type: none"> <li>Value of transactions in a month is more than [Z] percent of the average value for the client (or client profile)</li> </ul>
15	TM3.3 - Sudden increase in number of transactions in a month for the client	<ul style="list-style-type: none"> <li>Number of transactions in a month is more than [Z] percent of the average number for the client (or client profile)</li> </ul>
16	TM4.1 - High value transactions in a new account	<ul style="list-style-type: none"> <li>Transactions greater than INR [X] in newly opened account within [Y] months</li> </ul>
17	TM4.2 - High activity in a new account	<ul style="list-style-type: none"> <li>Number of transactions more than [N] in newly opened account within [Y] months</li> </ul>
18	TM5.1 - High value transactions in a dormant account	<ul style="list-style-type: none"> <li>Transactions greater than INR [X] in dormant account within [Y] days of reactivation</li> </ul>
19	TM5.2 - Sudden activity in a dormant account	<ul style="list-style-type: none"> <li>Number of transactions more than [N] in dormant account within [Y] days of reactivation</li> </ul>
20	TM6.1 - High value cash transactions inconsistent with profile	<ul style="list-style-type: none"> <li>Cash transactions greater than INR[X] by customer with low cash requirements such as Students, Housewife, Pensioners, Wages and salary Person and Minor Accounts</li> </ul>
21	TM6.2 - High cash activity	<ul style="list-style-type: none"> <li>Number of cash transactions greater than [X] by</li> </ul>



S. No.	Alert Indicator	Indicative Rule / Scenario
	inconsistent with profile	customer with low cash requirements such as Students, Housewife, Pensioners, Wages and salary Person and Minor Accounts
22	TY1.1 - Splitting of cash deposits just below INR 10,00,000 in multiple accounts in a month	<ul style="list-style-type: none"> <li>Cash deposits in amounts ranging between INR 9,00,000/- to INR 9,99,999.99) in multiple accounts of the customer greater than [N] times in a month</li> </ul>
23	TY1.2 - Splitting of cash deposits just below INR 50,000	<ul style="list-style-type: none"> <li>Deposit of cash in the account in amounts ranging between INR 40,000/- to INR 49,999/- greater than [N] times in [Y] days</li> </ul>
24	TY1.4 - Routing of funds through multiple accounts	<ul style="list-style-type: none"> <li>Transactions greater than INR[X1] between more than[N] accounts aggregating to more than[X2] on the same day</li> </ul>
25	TY1.5 - Frequent low cash deposits	<ul style="list-style-type: none"> <li>Cash deposits in amounts ranging between INR [X1] to [X2] greater than [N] times in [Y] days</li> </ul>
26	TY1.6 - Frequent low cash withdrawals	<ul style="list-style-type: none"> <li>Cash withdrawals in amounts ranging between INR [X1] to [X2] greater than [N] times in [Y] days</li> </ul>
27	TY2.1 - Many to one fund transfer	<ul style="list-style-type: none"> <li>Funds sent by more than [N] remitters to one recipient</li> </ul>
28	TY2.2 - One to many fund transfer	<ul style="list-style-type: none"> <li>Funds sent by one remitter to by more than [N] recipients</li> </ul>
29	TY3.1 - Customer providing different details to avoid linkage	<ul style="list-style-type: none"> <li>Customer provided different IDs or Date of Birth at different instances</li> </ul>
30	TY3.2 - Multiple customers working together	<ul style="list-style-type: none"> <li>Common address/telephone used by multiple unrelated customers</li> <li>Common IDs used by multiple customers</li> <li>Group of individuals conducting transactions at the same time</li> </ul>
31	TY4.1 - Repeated small cash deposits followed by immediate ATM withdrawals in different location	<ul style="list-style-type: none"> <li>Cash deposits in amounts ranging between INR [X1] to [X2] greater than [N] times in [Y] days followed by immediate ATM withdrawals in different location</li> </ul>
32	TY4.2 - Repeated small value transfers from unrelated parties	<ul style="list-style-type: none"> <li>Account to account transfer (RTGS/ NEFT) from unrelated parties in amounts ranging between INR</li> </ul>

S. No.	Alert Indicator	Indicative Rule / Scenario
	followed by immediate ATM withdrawals	[X1] to [X2] greater than [N] times in [Y] days followed by immediate ATM withdrawals
33	TY4.3 - Repeated small value inward remittance from unrelated parties followed by immediate ATM withdrawals	<ul style="list-style-type: none"> <li>Inward remittance (especially from high risk countries) from unrelated parties in amounts ranging between INR [X1] to [X2] greater than [N] times in [Y] days followed by immediate ATM withdrawals (especially other banks' ATMs)</li> </ul>
34	TY4.5 - Repeated small value inward remittance from unrelated parties used for specified activities	<ul style="list-style-type: none"> <li>Inward remittance (especially from high risk countries) used for purchase of communication equipments, tickets, hotel booking etc.</li> </ul>
35	TY5.1 - Majority of repayments in cash	<ul style="list-style-type: none"> <li>Card repayments greater than INR [X] amount in cash in [Y] days</li> <li>Card repayment in cash is greater than [Z] percent of repayments in [Y] days</li> </ul>
36	TY5.2 - Large debit balance in credit card	<ul style="list-style-type: none"> <li>Debit balance in credit card is greater than INR[X]</li> </ul>
37	TY5.3 - Large value card transactions for purchase of high value goods	<ul style="list-style-type: none"> <li>Card usage greater than INR [X] for jewellery (MCC 5944) in [Y] days</li> </ul>
38	TY5.4 - Large value cash withdrawals against international card	<ul style="list-style-type: none"> <li>Cash withdrawals greater than INR [X] against international card in [Y] days</li> </ul>
39	TY5.5 - Repeated small value cash withdrawals against international card	<ul style="list-style-type: none"> <li>Cash withdrawals against international card in amounts ranging between INR [X1] to [X2] greater than [N] times in [Y] days in locations with known terrorist incidents</li> </ul>
40	TY5.6 - Large repetitive card usage at the same merchant	<ul style="list-style-type: none"> <li>More than [N] transactions at same merchant aggregating to more than INR [X] in [Y] days</li> </ul>
41	TY7.1 - Repayment of loan in cash	<ul style="list-style-type: none"> <li>Loan repayments in cash greater than INR [X] in [Y] months</li> </ul>
42	TY7.2 - Premature closure of large FDR through PO/DD	<ul style="list-style-type: none"> <li>Premature closure of FDR for amount greater than INR [X] within [N] days and payment by PO/DD</li> </ul>
43	TY7.3 - High number of cheque leaves	<ul style="list-style-type: none"> <li>Greater than [X1] number cheque leaves issued for savings bank account and [X2] number of cheque</li> </ul>



S. No.	Alert Indicator	Indicative Rule / Scenario
		leaves issued for Current account in a period of [Y] days
44	TY7.4 - Frequent locker operations	• Number of locker operations greater than [X] times in [Y] days
45	RM1.1 - High value transactions by high risk customers	• Transactions greater than INR [X] by high risk customers
46	RM1.2 - High value cash transactions in NPO	• Cash transactions greater than INR [X] in Trust/NGO/NPO in [Y] days
47	RM1.3 - High value cash transactions related to real estate	• Cash transactions greater than INR [X] related to real estate transactions in [Y] days
48	RM1.4 - High value cash transactions by dealer in precious metal or stone	• Cash transactions greater than INR [X] by dealer in precious metal, precious stone or high value goods in [Y] days
49	RM2.2 - High value inward remittance	• Inward remittance greater than [X] value aggregated in [Y] days
50	RM2.3 - Inward remittance in a new account	• Inward remittance greater than [X] value in a new account within [Y] days
51	RM2.4 - Inward remittance inconsistent with client profile	• Inward remittance greater than [X] value in [Y] days in account of Students, Housewife, Pensioners, Wages and salary Person and Minor Accounts
52	RM3.1 - High value transactions with a country with high ML risk	• Transaction greater than INR [X] involving a country considered to be high risk from the money laundering or drug trafficking perspective.
53	RM3.2 - High value transactions with tax havens	• Transaction greater than INR [X] involving tax havens or countries that are known for highly secretive banking and corporate law practices.
54	RM4.1 - Transaction involving a country with high TF risk	• Transaction involving a country considered to be high risk from the terrorist financing perspective.



ILLUSTRATIVE EXAMPLES OF 'GROUNDS OF SUSPICION'

The following are some of the illustrative examples of 'Grounds of suspicion' which may lead to a conclusion about the suspicious nature of the transaction (these are covered by the RBI in its various circulars or IBA guidelines)

- i) If a branch has reason to believe that a customer is intentionally structuring any transaction into a series of transactions below the threshold of Rs.50000/- (Rupees fifty thousand). The branch should verify identity and address of customer and also consider filing a Suspicious Transaction Report (STR).
- ii) In the circumstances when a branch believes that it would no longer be satisfied that it knows the true identity of the account holder, the branch should also file an STR.
- iii) Branches should pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the branch. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. **High-risk** accounts have to be subjected to intensified monitoring.
- iv) Branch should exercise ongoing due diligence with respect to the business relationship with every client & closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds.
- v) If a branch has reason to believe that a customer is intentionally structuring wire transfer to below Rs.50000/- (Rupees fifty thousand) to several beneficiaries in order to avoid reporting or monitoring, the branch must insist on complete Customer Identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and STR should be made.
- vi) Wire transfers lacking complete originator information shall be identified and this must be considered as a factor in assessing whether a wire transfer or related transactions are suspicious. If they are found to be of suspicious nature then STR to be created.
- vii) "Money Mules" can be used to launder the proceeds of fraud schemes (e.g. phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "Money Mules." The operations of mule accounts can be minimized if branches follow the guidelines contained in the RBI Circulars on KYC. Branches are, therefore, advised to strictly adhere to the guidelines on KYC issued and to those relating to periodical updation of Customer Identification data after the account

- is opened. Branches are also required to monitor transactions in order to protect themselves and their customers from misuse by such fraudsters.
- viii) Branches are required to apply enhanced due diligence measures on 'high' and 'medium' risk customers. Accordingly, branches are also required to subject these 'high and medium risk accounts' to intensified transaction monitoring. Higher risk associated with such accounts should be taken into account by the branches to identify suspicious transactions for filing STRs.
  - ix) It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. The branches should report all such attempted transactions in STRs, even if not completed by customers. These should be reported irrespective of the amount of the transaction. Branches should raise STRs if they have reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences
  - x) The transactions that give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism should also be reported.
  - xi) When a business relationship is already in existence & it is not possible to perform Customer Due Diligence on the customer in respect of the business relationship STR to be created.
  - xii) Accounts of persons under investigation by any regulatory authority should be reported as suspicious.
  - xiii) It is imperative that the bank has a system in place, which will ensure that the account of the person of any dubious back ground is not opened or any suspicious transaction if routed through the branch will be identified. The CIP module of the AML package throws the alerts, if the name of the accountholder is similar to the name of the persons enumerated in the various lists uploaded in the system (UN sanctioned Terrorist list, Mumbai Police List, RBI cautioned list of exporters). If the branches are unable to establish if the true identity of the account holder is different from the name appearing in the list, then the same need to be reported as STR.

**Subjective test for identifying suspicious transactions:**

The review of pattern of transactions in the account and other related information provides an insight into intended purpose of the transaction. Examples where such review can assist in meeting the subjective test that 'gives rise to reasonable ground of suspicion' is as follows:

- i) Transaction pattern are not consistent with normal business, personal, remittance or tourist spending activity. For eg: High value transactions in the account of a maid servant, tailor etc.;

- ii) The amounts or frequency or the stated reason of the transaction does not make proper business sense or not commensurate with the profile of the customer, say student, etc.;
- iii) Large number of transfers received at once or over a certain period of time which is much greater than what would be expected for such a receiver;
- iv) Unrelated sender or receiver;
- v) Customer who travels unexplained distances to conduct transactions;
- vi) Migrant remittances made outside the usual remittance corridors;
- vii) Personal funds sent at a time not associated with salary payments;
- viii) Several accounts with same authorized signatories/introducer;
- ix) Cash deposited and transferred to own account with other bank or viceversa;
- x) Property transactions though cheque/RTGS in a newly opened account;
- xi) Walk in customer especially saying that he does not have any bank account till date;
- xii) It should be ensured that the business transactions are not routed through other than the business accounts. eg: Business transactions routed through savings account should be treated as suspicious.



## Appendix D

### Details of the element of Suspicion in the **new reporting** format

Element	Description	Length	Mandato.
Source Of Alert	<p>Source of alert for initiation of the STR.</p> <p>Permissible values are:            CV – Customer Verification            WL - Watch List            TY - Typology            TM - Transaction Monitoring            RM - Risk Management System            MR - Media Reports            LQ - Law Enforcement Agency Query            EI - Employee Initiated            PC- Public Complaint            BA – Business Associates            ZZ - Others            XX - Not Categorised</p>	2	Yes
Alert Indicator	<p>Red Flag indicator which had generated alert resulting in STR.</p> <p>The reporting entity may use a standard language of the red flag indicator. The reporting entity may use the language used in the instructions of the regulator or communication of FIU-IND.</p> <p>One STR can have more than one Alert Indicator. In the XML format more than one indicator can be mentioned for a report. In the fixed text format, the number of indicators for a report is limited to three.</p>	100	No
Suspicion Due To Proceeds Of Crime	<p>Whether the suspicion is on account of clause (a) of Rule 2(1) (g) relating to proceeds of an offence specified in the Schedule to the Act, regardless of the value involved.</p> <p>Permissible values are:            Y- Yes            N- No            X – Not categorised</p> <p>One STR may be related to more than one clause.</p>	1	Yes
Suspicion Due To Complex Trans	<p>Whether the suspicion is on account of clause (b) of Rule 2(1) (g) relating to circumstances of unusual or unjustified complexity.</p> <p>Permissible values are:            Y- Yes            N- No            X – Not categorised</p> <p>One STR may be related to more than one clause.</p>	1	Yes

<i>Element</i>	<i>Description</i>	<i>Length</i>	<i>Mandate</i>
Suspicion Due To Non Economic Rationale	<p>Whether the suspicion is on account of clause (c) of Rule 2(1) (g) relating to no economic rationale or bonafide purpose.</p> <p>Permissible values are: Y- Yes N- No X – Not categorised</p> <p>One STR may be related to more than one clause.</p>	1	Yes
Suspicion Of Financing Of Terrorism	<p>Whether the suspicion is on account of clause (d) of Rule 2(1) (g) relating to financing of the activities relating to terrorism.</p> <p>Permissible values are: Y- Yes N- No X – Not categorised</p> <p>One STR may be related to more than one clause.</p>	1	Yes
Attempted Transaction	<p>Whether the STR relates to an attempted transaction that was not completed. Permissible values are: Y- Yes N- No X – Not categorised</p>	1	Yes
Grounds Of Suspicion	<p>Summary of suspicion and sequence of events covering following aspects:</p> <ul style="list-style-type: none"> <li>• Background/profile/occupation of the customer and other related individuals/entities.</li> <li>• When did the relationship with the customer begin?</li> <li>• How was suspicion detected?</li> <li>• What information was linked or collected during the review process?</li> <li>• What explanation was provided by the subject(s) or other persons (without tipping off)?</li> <li>• Summary of suspicion</li> <li>• Whether the suspicious activity is an isolated incident or relates to another transaction?</li> <li>• Who benefited, financially or otherwise, from the transaction(s), how much, and how (if known)?</li> <li>• What is the volume of transactions in reported accounts in the financial year, and what is the volume of cash transactions?</li> <li>• Whether any STR filed for the customer earlier?</li> <li>• Any additional information that might assist law enforcement authorities.</li> </ul>	4000	Yes

<i>Element</i>	<i>Description</i>	<i>Length</i>	<i>Mandato</i>
Details Of Investigation	<p>Details about investigation being conducted covering the name of agency, contact person and contact details.</p> <p>The investigation could be both internal to the reporting entity or any investigation by law enforcement agency. In case of law enforcement agency the details of contact person needs to be separately furnished under LEA Details below.</p>	4000	No
LEA Informed	<p>Whether any Law enforcement agency is informed about the incident reported in the STR.</p> <p>Permissible values are:  R - Information received  S - Information sent  N - No correspondence sent or received  X - Not categorised.</p> <p>Refer section 11.1.7.2 for further details on enumerations.</p>	1	Yes
LEA Details	<p>Contact details of person in the law enforcement agency which is conducting the investigation.</p> <p>The details of the investigation should be furnished under Details Of Investigation above.</p>	250	No
Priority Rating	<p>Priority attached to the report as per assessment of the reporting entity.</p> <p>Permissible values are:  P1- Very High Priority  P2- High Priority  P3- Normal Priority  XX- Not categorised</p> <p>The reporting entity can attach P1 priority for reports which requires immediate attention of FIU. Refer section 11.1.7.3 for further details on enumerations.</p>	2	Yes
Report Coverage	<p>Whether all the suspicious transactions are covered or a sample set is being reported?</p> <p>Permissible values are:  C - Complete  P - Partial  X - Not categorised</p> <p>Refer section 11.1.7.4 for further details on enumerations.</p>	1	Yes



<i>Element</i>	<i>Description</i>	<i>Length</i>	<i>Mandatory</i>
Additional Documents	<p>Whether the reporting entity wants to submit additional documents separately for the STR.</p> <p>Permissible values are:  Y - Yes  N - No  X - Not categorised</p> <p>The reporting entity can't upload additional documents with the report. They will be sent a separate request for providing additional information.</p>	1	Yes

## Appendix E

### Indicative List of High / Medium risk customers

The following lists are indicative and can be expanded. The banks have the option to upgrade the risk categorisation (i.e. medium to high) for any specific industry / segment.

### Characteristics of High Risk Customers

1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.;
2. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities;
3. Individuals and entities in watch lists issued by Interpol and other similar international organizations;
4. Customers with dubious reputation as per public information available or commercially available watch lists;
5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;
6. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.;
7. Customers based in high risk countries/jurisdictions or locations (refer Appendix G);
8. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
9. Non-resident customers and foreign nationals;
10. Embassies / Consulates;
11. Off-shore (foreign) corporation/business;
12. Non face-to-face customers;
13. High net worth individuals;
14. Firms with 'sleeping partners' ;
15. Companies having close family shareholding or beneficial ownership ;
16. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;

17. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence;
18. Investment Management / Money Management Company/Personal Investment Company;
19. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution;
20. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc;
21. Trusts, charities, NGOs/NPOs (especially those operating on a "cross-border" basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies);
22. Money Service Business: including seller of: Money Orders / Travelers' Checks / Money Transmission / Check Cashing / Currency Dealing or Exchange;
23. Business accepting third party checks (except supermarkets or retail stores that accept payroll checks/cash payroll checks);
24. Gambling/gaming including "Junket Operators" arranging gambling tours;
25. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers);
26. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries);
27. Customers engaged in industries that might relate to nuclear proliferation activities or explosives;
28. Customers that may appear to be Multi level marketing companies etc.

#### **Characteristics of Medium Risk Customers**

1. Non-Bank Financial Institution;
2. Stock brokerage;
3. Import / Export;
4. Gas Station;
5. Car / Boat / Plane Dealership;
6. Electronics (wholesale);



7. Travel agency;
8. Used car sales;
9. Telemarketers;
10. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center;
11. Dot-com company or internet business;
12. Pawnshops;
13. Auctioneers;
14. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.;
15. Sole Practitioners or Law Firms (small, little known);
16. Notaries (small, little known);
17. Secretarial Firms (small, little known);
18. Accountants (small, little known firms);
19. Venture capital companies.

## Appendix F

### Indicative List of High / Medium risk Products & Services

1. Electronic funds payment services such as Electronic cash (e.g., stored value and payroll cards), funds transfers (domestic and international), etc
2. Electronic banking
3. Private banking (domestic and international)
4. Trust and asset management services
5. Monetary instruments such as Travelers' Cheque
6. Foreign correspondent accounts
7. Trade finance (such as letters of credit)
8. Special use or concentration accounts
9. Lending activities, particularly loans secured by cash collateral and marketable securities
10. Non-deposit account services such as Non-deposit investment products and Insurance
11. Transactions undertaken for non-account holders (occasional customers)
12. Provision of safe custody and safety deposit boxes
13. Currency exchange transactions
14. Project financing of sensitive industries in high-risk jurisdictions
15. Trade finance services and transactions involving high-risk jurisdictions
16. Services offering anonymity or involving third parties
17. Services involving banknote and precious metal trading and delivery
18. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.