

## بررسی نقش مبارزه با پول شویی مبتنی بر رویکرد ریسک محور در خدمات نوین بانکی

هیدی یوسفی، \* جمیله پیکر \*\*

### چکیده

امروزه «پول شویی» به عنوان مفهومی با کاربرد وسیع در سیستم‌های اقتصادی ملل مختلف مطرح شده و بانک‌ها به عنوان یکی از پرکاربردترین درگاه‌های فعالیت پول شویان، قسمت اصلی معاملات مالی مربوط به دارایی‌های حاصل از فعالیت‌های سازمان یافته غیرقانونی را به خود اختصاص داده‌اند. همزمان با رشد روز افزون خدمات مالی، جرایم مالی نیز با پیچیدگی‌های فزاینده‌ای در حال رشد هستند. این در حالی است که عموماً سیستم‌های نظارتی و کنترلی، دارای سرعت رشد به نسبت پایین‌تری هستند. در چنین شرایطی، لزوم بررسی‌های دقیق نهادهای مالی، محصولات و خدمات مالی، نظارت‌ها و کنترل‌های مستمر و ارائه راهکارهای هوشمند در مقابله با جرایم مالی و تروریسم، بیش از پیش احساس می‌شود. از سوی دیگر، به دلیل وجود بازار رقابتی شدید ارائه خدمات در میان بانک‌های ایران و گسترش ارائه خدمات نوین الکترونیکی، ریسک پول شویی در این بخش از نهادها به شدت رو به افزایش بوده و حتی در بسیاری از موارد، بانک‌ها به مکان مناسبی برای پول شویان تبدیل شده است. بدین ترتیب، مبارزه با پول شویی با رویکرد ریسک محور در محصولات الکترونیکی نوین، از اصلی‌ترین وظایف نهادهای مالی در حوزه مبارزه با پول شویی و تأمین مالی تروریسم به شمار می‌رود. در این مقاله سعی شده است، فرآیند مبارزه با پول شویی و تأمین مالی تروریسم با استفاده از رویکرد ریسک محور در خدمات نوین الکترونیکی، بر اساس رهنمودهای گروه ویژه اقدامات مالی (FATF)، با توجه به موقعیت و شرایط داخلی کشور ایران، مورد مطالعه قرار گیرد. این پژوهش، به ارائه چارچوبی برای شناسایی شرایط پرریسک و کم‌ریسک می‌پردازد که به منظور ارائه شاخص‌های ریسک پول شویی و تأمین مالی تروریسم به عنوان هدفی بلندمدت ضروری است. همچنین، انتظار می‌رود، پژوهش پیش‌رو، گامی اولیه برای شفاف‌سازی و لزوم تقویت قدرت نظارتی و کنترلی نهادهای ناظر این حوزه به منظور تعیین چارچوب نظارتی منسجم بردارد تا چارچوب مورد نظر، بر اساس استانداردهای FATF و شرایط حال حاضر کشور تعریف گردد.

واژگان کلیدی: خدمات نوین الکترونیکی، مبارزه با پول شویی، تأمین مالی تروریسم و شاخص‌های ریسک.

طبقه‌بندی JEL : R51 , G32 , K42.

\* کارشناس ارشد اقتصاد، رئیس اداره مدیریت ریسک و مبارزه با پول شویی بانک آینده hedi.yousefi@yahoo.com

\*\* کارشناس ارشد ریاضیات مالی، کارشناس اداره مدیریت ریسک و مبارزه با پول شویی بانک آینده jamileh.peykar@gmail.com

## ۱. مقدمه

پول‌شویان همواره تلاش می‌کنند به گونه‌ای رفتار نمایند که معاملات غیرمشموع آنها از عملیات مشموع قابل تمیز نباشد. بنابراین، بانک‌ها در مواجهه با پول‌شویان همواره با ریسک‌های قابل توجهی روبه‌رو هستند. از این رو می‌بایست برنامه مبارزه با پول‌شویی در بانک‌ها و مؤسسات اعتباری به نوعی تنظیم شود که امکان تفکیک معاملات غیرقانونی با عملیات قانونی را فراهم نمایند.<sup>۱</sup>

با توجه به پژوهش‌های بین‌المللی انجام شده در خصوص روش‌های نوین پول‌شویی، باید به این نکته توجه نمود که معمولاً پول‌شویان بیشتر از هر کارمند بانکی، از سیستم‌ها، فرآیندها، مشکلات و شکاف‌های موجود اطلاع دارند. آنها از کوچکترین شکاف‌های موجود در هر بخشی به‌منظور استفاده در راستای منافع خود بهره می‌برند. بنابراین، بررسی دقیق تمامی فرآیندها، آزمون تمامی محصولات، نظارت بر نقاط ضعف و اطمینان از مدیریت شکاف‌های موجود در سیستم، ریسک پول‌شویی را کاهش خواهد داد.<sup>۲</sup>

رویکرد ریسک‌محور مبارزه با پول‌شویی، دارای سناریویی مبتنی بر طبقه‌بندی ریسک است. بدین صورت که افراد، مناطق، مشاغل، زمان‌ها و شرایط دیگر ریسکی، شناسایی و طبقه‌بندی می‌شوند و بر اساس تحلیل‌های صورت‌گرفته سناریوهای کنترلی، تعیین یا بازبینی می‌شوند. اما به طور کلی هیچ روش‌شناسی استاندارد و جهان‌شمولی که مورد پذیرش تمامی دولت‌ها و مؤسسات بوده و بتواند ماهیت و میزان ریسک ناشی از عملیات پول‌شویان را مشخص نماید، وجود ندارد.

ساختار برنامه‌های ضد پول‌شویی باید مبتنی بر ریسک باشد. به این معنی که کنترل‌های مورد نیاز باید مبتنی بر ریسک مشتری، ریسک محصول یا خدمتی که به مشتری ارائه می‌شود و ریسک منطقه فعالیت بانک یا سازمان مالی باشد که به مشتری ارائه خدمت می‌کند. بانک‌ها باید قادر به اداره و هدایت برنامه ارزیابی ریسک خود باشند و اطمینان یابند که کنترل‌های اعمال شده، متناسب با سطح ریسک

۱. تذهیبی، (۱۳۸۹).

۲. بیابانی و عصار، (۱۳۸۸)، ص ۲۲۲ و ۲۴۳؛ پاکروان، (۱۳۸۹)، ص ۱۵۵.

مربوطه است. در این راستا، شناسایی محصولات پرریسک به عنوان یکی از مسیرهای احتمالی مورد استفاده توسط پول‌شویان بسیار حائز اهمیت است.<sup>۱</sup>

توجه به این نکته ضروری است که ریسک موارد خاص در هر مؤسسه با توجه به ماهیت فعالیت و عملیات آن مؤسسه، ارزیابی و اندازه‌گیری می‌شود. بنابراین، اندازه ریسک مشتری و معاملات انجام شده توسط وی، بر اساس عملیات مؤسسات مختلف، متغیر خواهد بود.

## ۲. ادبیات موضوع

### ۲-۱. تاریخچه موضوع

آنچه واضح به نظر می‌رسد این است که در حوزه رویکرد ریسک‌محور مبارزه با پول‌شویی، کار علمی و پژوهش‌های بنیادینی در داخل کشور ایران صورت نگرفته است. برگردان فارسی رویکردهای کمیته بال و FATF<sup>۲</sup> مرتبط با مبارزه با پول‌شویی مبتنی بر رویکرد ریسک‌محور و نظارت مبتنی بر ریسک، گام مهمی است که در این حوزه در داخل کشور و توسط اداره مبارزه با پول‌شویی بانک مرکزی ایران برداشته شده است. امید است، ادامه این مسیر به همراه مطالعات بیشتر در این حوزه، به تبیین چارچوب بومی مبارزه با پول‌شویی و تأمین مالی تروریسم مبتنی بر رویکرد ریسک‌محور و نظارت ریسک‌محور بیانجامد. این درحالی است که در خارج از ایران، کشورهای مختلف با بومی‌سازی رهنمودهای سازمان FATF و تجارب پرونده‌های پول‌شویی خود، توانسته‌اند چارچوبی برای رویکرد ریسک‌محور مبارزه با پول‌شویی تدوین نمایند. در این راستا می‌توان به پژوهش‌های دولت استرالیا<sup>۳</sup> و ساختار ارائه شده آنها اشاره کرد که در این مقاله نیز از آن استفاه شده است. مرکز مالی بین‌المللی دبی<sup>۴</sup>، دولت انگلیس (تیم سیاست اطلاعاتی)<sup>۵</sup>، بانک مرکزی نیجریه<sup>۶</sup> و بسیاری از سازمان‌های دولتی و بانک‌های مرکزی ملل مختلف در این رابطه پژوهش‌های متناسب با شرایط آن کشور را انجام داده و چارچوب خود را اعلام نموده‌اند. در این بین،

۱. مهجوریان، (۱۳۹۲).

2. Financial Action Task Force
3. Australian Government .( 2006).
4. Dubai International Financial Centre .(2013).
5. The Information Policy Team .(2012).
6. Central Bank of Nigeria. (2011).

برخی از شرکت‌های حوزه مالی نیز وارد این حیطه شده و کارهای ارزشمندی ارائه کرده‌اند. از جمله این پژوهش‌ها می‌توان به ارزیابی ریسک مشتریان<sup>۱</sup>، کاری از شرکت متاونت<sup>۲</sup> اشاره کرد که پس از بررسی ابعاد مختلف مؤثر بر رابطه مشتری با نهاد مالی و ویژگی‌های مختلف مشتریان، توانسته مدلی برای ارزیابی ریسک مشتریان برای سازمانهای مالی ارایه نماید.

در خصوص موضوع مپ/تت<sup>۳</sup> در داخل، سیزده دستورالعمل، یک آیین‌نامه و قانون تصویب و به بانک‌های ایرانی ابلاغ شده که در متن برخی از آنها به مباحث مرتبط به ریسک مشتری پرداخت شده است، که در زیر به آن اشاره می‌شود:

- دستورالعمل چگونگی شناسایی مشتریان ایرانی مؤسسات اعتباری،
- دستورالعمل نحوه اعمال دقت و نظارت ویژه هنگام ارائه خدمات پایه به اشخاص سیاسی خارجی در مؤسسات اعتباری،
- دستورالعمل چگونگی شناسایی مشتریان خارجی مؤسسات اعتباری،
- دستورالعمل لزوم رعایت مقررات مبارزه با پول‌شویی در روابط کارگزاری بانک‌های پوستانه‌ای.

با توجه به موارد پیش‌گفته و دستورالعمل‌های ویژه برای بررسی ریسک مشتری، برخی اقدام‌ها، در سطح تمام بانک‌ها الزامی بوده و متولیان نظارت بر نحوه عملکرد بانک‌ها نیز اداره مبارزه با پول‌شویی بانک مرکزی ایران، واحد اطلاعات مالی وزارت امور اقتصادی و دارایی (FIU) و ادارات مبارزه با پول‌شویی بانک‌ها هستند. از مهم‌ترین اقدام‌های صورت‌گرفته در حوزه مپ/تت و مرتبط با ریسک مشتری در ایران، وجود بسترهای استعلام هویتی اشخاص حقیقی و حقوقی کشور است. امکان احراز هویت با استفاده از سامانه‌های برخط<sup>۴</sup> و لزوم احراز هویت در زمان تعریف مشتری، افتتاح حساب و ارائه برخی خدمات بانکی دیگر است. در خصوص دیگر عملیات اجرایی مشترک شبکه بانکی کشور باید

1. Price .(2008).

2. Metavante

۳. مبارزه با پول‌شویی و یا تامین مالی تروریسم به اختصار مپ/تت نامیده می‌شود.

4. Online

به این نکته توجه شود که برنامه‌های نظارتی این حوزه، به شدت در حال رشد است. در این راستا می‌توان به بیان برخی موارد ذیل اکتفا نمود:

- ابلاغ فاز اول قواعد پول‌شویی و ارائه الگوریتم‌های اولیه جهت استخراج و نظارت بر تراکنش‌ها در سطح کلیه بانک‌ها
- تعیین سطح فعالیت مشتریان و پیاده‌سازی سامانه شهاب و نهاب
- جمع‌آوری و بررسی گزارش‌های واريز بیش از سقف مقرر و گزارش معاملات مشکوک به پول‌شویی، از سطح کلیه بانک‌ها در واحد اطلاعات مالی،
- استعلام‌های واحد اطلاعات مالی، بانک مرکزی و سایر نهادهای ذی‌صلاح در خصوص پرونده‌های مشکوک به پول‌شویی،
- به اشتراک‌گذاری فهرست افراد مظنون به پول‌شویی بین تمام بانک‌ها و واحد اطلاعات مالی،
- گزارش عملکرد حوزه مبارزه با پول‌شویی بانک‌ها به بانک مرکزی و واحد اطلاعات مالی.

## ۲-۲. ریسک چیست؟

ریسک می‌تواند به عنوان ترکیبی از یک رخداد و میزان عواقب آن رخداد، باشد.<sup>۱</sup> به عبارت ساده‌تر، ریسک می‌تواند به عنوان ترکیبی از شانسی که برخی مواقع ممکن است اتفاق افتد و درجه خطر یا زیانی که در نتیجه آن تحمیل می‌شود، باشد. در این مقاله منظور از ریسک، ریسک پول‌شویی و تأمین مالی تروریسم است.

## ۳-۲. مدیریت ریسک چیست؟

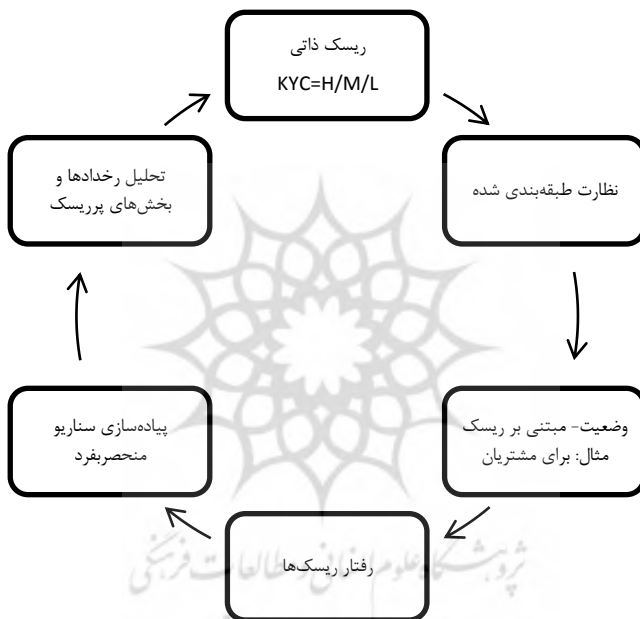
مدیریت ریسک، فرآیند تشخیص و توسعه روش‌هایی برای کاهش و مدیریت یک نوع ریسک است. این فرآیند مستلزم گسترش روش‌های تشخیص، اولویت‌بندی، درمان (مقابل با آن)، کنترل و نظارت بر میزان سرمایه در معرض خطر است. در اینجا هدف از مدیریت ریسک، مدیریت فرآیندی است که در آن، رخدادی

1. International Organisation for Standardisation. ISO/IEC Guide 73 Risk management ° Vocabulary ° Guidelines for Use in Standards. Geneva: ISO. (2002).

بر خلاف احتمال وقوع آن اتفاق می‌افتد و شدت مورد انتظار، میزان زیان یا خطری است که ممکن است در صورت وقوع رخداد یادشده تحمیل شود.

در این خصوص، در زیر فرآیند مدیریت ریسک مشتری شرکت SAS ارائه شده است. مراحل یادشده می‌بایست در تمامی ریسک‌ها پیاده‌سازی و بر اساس سیاست نهاد مربوطه، در بازه‌های زمانی معینی به روز رسانی شوند.

شکل ۱. فرآیند مدیریت ریسک پ/ت<sup>۲</sup> در شرکت SAS



مأخذ: SAS Institute. (2009), p. 8.

#### ۲-۴. کدامیک از ریسک‌ها نیاز به مدیریت دارند؟

در خصوص موضوع مپ/ت، به طور کلی انتظار می‌رود، مدیریت ریسک هر کسب و کار، دو ریسک اصلی را مدنظر داشته باشد:

1. Australian Government, Ibid. (2006).

۲. پول‌شویی / تامین مالی تروریسم به اختصار پ/ت نامیده می‌شود.

- **ریسک کسب و کار:** بدین معنی که ممکن است از کسب و کار شما در راستای اهداف مپ/ت استفاده شود.
- **ریسک نظارتی:** ریسک نظارتی، ارتباط و همبستگی زیادی به ضعف یا نبود پایبندی به تعهدات نسبت به برنامه‌های مپ/ت دارد. نمونه‌ای از این تعهدات و وظایف متداول، ممکن است کوتاهی در ارائه گزارش تراکنش‌های اصلی از قبیل دستورالعمل انتقال وجوه در سطح بین‌المللی، احراز هویت مشتریان و یا داشتن برنامه مپ/ت (نشان‌دهنده چگونگی کسب و کار مؤسسه در شناسایی و مدیریت ریسک پ/ت خود است) باشد.
- در فضای واقعی، وجود کسب و کار کاملاً بدون ریسک در موضوع پ/ت، امکان‌پذیر نیست. بنابراین، فرض می‌شود که هر کسب و کار، ریسک پ/ت مربوط به خود را شناسایی کرده و سپس، سعی در یافتن بهترین روش به منظور کاهش و مدیریت آن داشته باشد. بدین منظور، ایجاد تعادلی بین هزینه هر کسب و کار و مشتریان آن در مقابل ریسک پ/ت که آن کسب و کار با آن روبه‌روست، ضروری است. گفتنی‌است، این امر، متناسب با اندازه کسب و کار و منابع در دسترس مؤسسه خواهد بود. بدین ترتیب، یک کسب و کار خاص، می‌تواند آن دسته از ریسک پ/ت را کنترل کند که انتظار روبه‌رویی با آن را در زمان ارائه خدمات و یا تولید محصولات در نظر گرفته باشد.
- در اجرای کامل فرآیند ریسک‌محور مبارزه با پول‌شویی و تأمین مالی تروریسم لازم است ابتدا با استفاده از یک استاندارد خاص و یا تعریف یک چارچوب ویژه، و ضمن آگاهی از شرایط محدوده قضایی، انواع طبقات ریسک پ/ت مورد مطالعه قرار گرفته و اجرایی شود. در اینجا برای آشنایی بیشتر، طبقه‌های ریسک پ/ت و زیرشاخه‌های هر یک، در استاندارد کشور استرالیا بیان می‌شود:
- ریسک شناسایی
  - ریسک مشتری،
  - ریسک محصولات و خدمات،
  - ریسک شیوه‌های ارائه خدمات و محصولات / ریسک روش‌های انجام کار،
  - ریسک حوزه قضایی یا کشور مربوطه.

- ریسک ارزیابی و اندازه‌گیری
    - درست‌نمایی- شانس رخداد ریسک،
    - اثر- میزان زیان یا خطر در صورت رخداد ریسک،
    - درست‌نمایی\* اثر= درجه یا رتبه ریسک،
    - ریسک درمان.
  - مدیریت ریسک کسب و کار
    - مدیریت و کمینه نمودن ریسک،
    - کاربرد راهبرها، سیاست‌ها و رویه‌ها.
  - مدیریت ریسک نظارت
    - جایگذاری صحیح سیستم‌ها و کنترل‌ها،
    - اجرای طرح مدیریت ریسک و برنامه مپ/تت.
  - ریسک نظارت و بازنگری
    - توسعه و پیاده‌سازی فرآیند نظارت،
    - نگهداری مدارک و پیشینه‌های ضروری،
    - بازنگری طرح ریسک و برنامه مپ/تت،
    - حسابرسی داخلی یا ارزیابی،
    - ارائه گزارش‌ها بر اساس مپ/تت.
- به عنوان مرحله اول و پایه‌ای، تمرکز اصلی این مقاله، ریسک شناسایی است. در این راستا، انتظار می‌رود در نخستین گام، هر کسب و کار، چهار گروه زیر را به منظور ارزیابی ریسک شناسایی خود، مورد مطالعه قرار دهد.<sup>۱</sup>

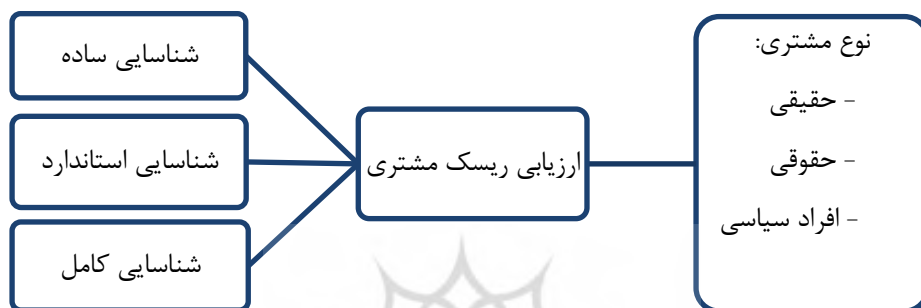
1. Australian Government, Ibid. (2006).



## ۲-۴-۱. ریسک مشتری

بر اساس قوانین داخلی و استانداردهای بین‌المللی، سطوح مختلف شناسایی برای گروه‌های مختلف مشتریان وجود دارد که در جدول زیر می‌توان مشاهده کرد.<sup>۱</sup>

شکل ۲. ارزیابی ریسک مشتری



به منظور دسته‌بندی مشتریان از منظر ریسک پ/ت، شناسایی و طبقه‌بندی آنها از این حیث، امری اجتناب‌ناپذیر است. در این راستا، در سطح بین‌المللی، حوزه‌های قضایی مختلف اقدام به تعیین استاندارد جامع به منظور شناسایی دقیق مشتریان و تفکیک طبقه‌های مختلف ریسکی نموده‌اند. در این خصوص، به صورت کلی دسته‌های زیر به عنوان مشتریان پرریسک شناسایی می‌شوند:<sup>۲</sup>

- مشتریان جدید،
- مشتریان جدیدی که می‌خواهند تراکنش‌های با تعداد یا مبالغ به نسبت بالا داشته باشند،
- یک مشتری یا گروهی از مشتریان که تراکنش‌های زیادی با یک مشتری یا گروهی از مشتریان خاص دارند،
- مشتری‌ای که احراز هویتشان با مشکلاتی روبه‌رو است،
- مشتری‌ای که مقدار زیادی اسکناس و یا پول خرد برای واریز به شعب می‌آورد.
- مشتریان دارای مشاغل پرخطر

۱. ارجمندزاد و کاظمیان، (۱۳۹۲).

2. Australian Government, Ibid. (2006).

### - مشتریان فعال در حوزه‌های جغرافیایی پرخطر

پژوهش‌های صورت گرفته در استرالیا، نیجریه، پاکستان و نهادها و شرکت‌های بین‌المللی نشان دهنده این واقعیت است که، جزئیات طبقه‌بندی‌ها، روش‌های کمی‌سازی، روش‌های رتبه‌بندی ریسک پ/ت مشتریان و تعیین سطح کنترلی برای هر طبقه، در هر حوزه قضایی متفاوت است. از یک سو، در بیشتر کشورهای پیشرو در حوزه پ/ت، اطلاعات معتبر و موثقی از وضعیت هویتی و رفتار مالی مشتری وجود دارد که می‌تواند پشتوانه تحقیقات متخصصان حوزه مپ/ت جهت ارزیابی ریسک مشتریان باشد. از سوی دیگر، فرهنگ شفاف‌سازی اطلاعات در این کشورها یکی از عوامل تاثیرگذار در مسیر موفقیت آنها در اجرای برنامه‌های مپ/ت است. لذا پرواضح است که ضعف در دو مورد مذکور جزء موثرترین موانع و چالش‌های پیش‌روی برنامه‌های نظارتی و مدیریتی حوزه مپ/ت در ایران است.

تعیین سطح فعالیت مشتریان و شناسایی ریسک انواع مشتریان از منظر پ/ت یکی از الزامات ایجاد بستری از محدودیت به منظور مبارزه با پولشویی مبتنی بر رویکرد ریسک محور است. با توجه به مشکلات موجود در این مسیر (در ایران)، به نظر می‌رسد، در چنین شرایطی یکی از روش‌های جایگزین، اکتفا به خوداظهاری مشتریان حقیقی/ حقوقی و استفاده از حداقل داده‌های معتبر از جمله سابقه مشتری نزد بانک باشد.

### ۲-۴-۲. ریسک کشور

در خصوص میزان و اندازه ریسک کشورها نیز توافق جهانی وجود ندارد؛ به‌ویژه در حوزه مبارزه با تروریسم. بدین معنی که ممکن است هر کشور یا حوزه قضایی، بنا به گرایش‌های سیاسی خود، برخی از فعالیت‌های یک حوزه قضایی را کم‌خطر و کشور دیگر، همان فعالیت‌های مالی را مصداق اقدام‌های تروریستی قلمداد کند؛ اما با یک نگرش کلی می‌توان گفت که عوامل مؤثر در پر ریسک بودن هر کشور از منظر پول‌شویی و تأمین مالی تروریسم، به شرح زیر است:

- کشورهای مشمول تحریم یا اقدام‌های مشابه از سوی سازمان ملل و نظایر آن،
- کشورهایی که FATF آنها را به عنوان غیر همکار معرفی می‌نماید،

- کشورهای که سازمان‌ها و منابع معتبر، آنها را حامی تروریسم معرفی می‌نمایند،
  - کشورهای که سطح بالایی از فساد و یا فعالیت‌های خرابکارانه در آنها توسط منابع معتبر گزارش می‌شود.<sup>۱</sup>
  - کشورهای داری نظام مالی و مالیاتی غیر یکپارچه و غیر شفاف
- در ایران نیز، فهرست کشورها و مناطق پرخطر از طریق بانک مرکزی و واحد اطلاعات مالی وزارت امور اقتصادی و دارایی اعلام می‌شود. تمامی بانک‌ها موظف‌اند بسته به سطح ریسک اعلام‌شده برای هر کشور، برخورد متناسبی داشته و ملاحظات متناسبی را اتخاذ نمایند.<sup>۲</sup>

## ۲-۴-۳. ریسک محصول

شناسایی ریسک خدمات مؤسسات مالی به ارزیابی کامل‌تری از سطح ریسک آنها منجر می‌شود. در این ارزیابی باید خدمات پریسک مشخص شده و در شیوه کلی رویکرد ریسک محور، مد نظر قرار گیرد. به‌ویژه در رویکرد ریسک محور، باید خدمات نوینی که مؤسسات به‌طور کامل آنها را ارائه نداده‌اند و یا برای ارائه بخشی یا کل آن خدمات، از خدمات مؤسسات دیگری استفاده می‌نمایند، به‌طور دقیق ارزیابی شوند؛ زیرا نظارت و کنترل چنین محصولاتی بسیار پیچیده‌تر و در مواردی بسیار پرهزینه خواهد بود.

افزون بر این، خدماتی که قابلیت تراکنش‌های برخط را دارند، ریسک بیشتری دارند.<sup>۳</sup> بدین منظور نظارت بر موقعیت جغرافیایی / مکان تراکنش‌ها و تغییرات در اندازه و جوه از حساسیت بالایی در این گروه از خدمات، برخوردارند. از میان خدمات پریسک دیگر، می‌توان به انتقال جوه از طریق بانک‌های کارگزار و روابط بانکی خصوصی<sup>۴</sup> (ارائه محصولات مالی به شکل خصوصی به مشتریان خاص) نیز اشاره کرد. به نظر می‌رسد بانک‌هایی با فعالیت‌های پیچیده‌تر که درگیر نقل و انتقالات برون مرزی هستند و یا تمرکز خود را بر خدمات بانکی اختصاصی گذاشته‌اند، در معرض ریسک بیشتری از منظر

1. Australian Government, Ibid. (2006).

۲. مهجوریان. (۱۳۹۲)؛ ارجمندنژاد و کاظمیان. (۱۳۹۲).

3. State Bank of Pakistan. (2012).

4. Private Banking Relationships

پ/ت باشند، بنابراین، از منظر رویکرد ریسک‌محور، می‌بایست تحت نظارت و بازرسی بیشتری قرار گیرند.<sup>۱</sup>

گفتنی است، در حال حاضر برخی خدمات پریسک مانند امکان انتقال وجوه از طریق بانک‌های کارگزار در بانک‌ها و مؤسسات مالی ایران امکان‌پذیر نیست. بدین‌روی، در حال حاضر محدودیت‌های مورد بحث در این خصوص در سیستم بانکی ایران صادق نخواهد بود. در حالی که در ادبیات این موضوع، ریسک م/پ در رابطه با تراکنش‌های صورت‌گرفته از طریق بانک‌های کارگزار و بانک‌های پوسته‌ای بخش مهمی را به خود اختصاص می‌دهند.

به منظور ارزیابی ریسک محصولات، باید نگاه ویژه‌ای به بانکداری الکترونیکی داشت. زیرا این دسته از خدمات و محصولات، نسبت به فعالیت‌های پول‌شویی بسیار آسیب‌پذیر است. علت آن نیز سرعت بالا، گستره وسیع جغرافیایی انجام عملیات و امکان گمنام ماندن کاربران خدمات بانکداری الکترونیکی است.<sup>۲</sup> در خصوص خدمات قابل ارائه در این حوزه در ایران می‌توان به اینترنت بانک، همراه بانک و تلفن بانک و ... اشاره کرد. به دلیل رشد روزافزون این نوع از خدمات و نیاز حوزه بانکی به بررسی ریسک‌های نوین و ناشناس این حوزه، در ادامه این پژوهش به مقوله خدمات الکترونیکی و ریسک‌های پ/ت این حوزه پرداخته می‌شود.

## ۲-۵. محدوده و محدودیت

ایجاد محدوده و محدودیت، به‌ویژه بر روی تراکنش‌های مالی، به عنوان یکی از ابزارهای مناسب برای مدیریت ریسک محصولات و خدمات در نهادهای مالی بزرگ مطرح می‌شود. باید دقت شود که ممکن است ایجاد چنین محدودیت‌هایی برای نهادهای مالی کوچک و متوسط کارا نباشد. در این راستا، انتظار می‌رود، هر نهاد مالی شیوه‌ای را انتخاب کند که متناسب با کسب و کار (از نظر اندازه، ماهیت و پیچیدگی) و ریسک‌های پول‌شویی و تأمین مالی تروریسم (پ/ت) ویژه همان نهاد مالی باشد. امکان

۱. کشتکار. (۱۳۹۳).

2. FATF. (2010).

ایجاد چنین محدودیت‌هایی، نیازمند وجود بستری مناسب از جمله وجود فضای شفافیت از وضعیت مالی نهادهای مالی و انواع مشتریان خواهد بود.

### ۳. روش پژوهش

روش این پژوهش، تحقیق و توسعه است؛ زیرا چارچوب مورد نظر این مقاله با تکیه بر گزارش ۲۰۱۰ سازمان FATF<sup>۱</sup> تهیه و تنظیم شده است. همچنین، با توجه به قوانین داخلی این حوزه، ساختارها و چارچوب‌های اولیه‌ای ارائه و بررسی شده است. بدین ترتیب، این پژوهش از نوع کاربردی محسوب می‌شود. در این مقاله، پس از بررسی شاخص‌های پیاده‌سازی شده در انواع حوزه‌های قضایی، برخی از شاخص‌های متناسب با وضعیت موجود در کشور ایران انتخاب شده و عوامل مؤثر در تنظیم "چارچوب رویکرد ریسک‌محور در خدمات نوین بانکی" مطرح می‌شود.

### ۳-۱. ارزیابی ریسک خدمات الکترونیکی

در گزارش‌های سازمان FATF، ویژگی‌های مشترک خدمات نوین الکترونیکی که باعث رونق استفاده از این خدمات در مقابل خدمات سنتی و نقدی شده است، به شرح زیر است:<sup>۲</sup>

- نبود ریسک اعتباری،
- سرعت بالای تراکنش،
- امکان ارتباط‌های تجاری غیر حضوری.

برخلاف پول نقد، خدمات نوینی که با استفاده از تکنولوژی‌های روز ارائه می‌شوند، تراکنش‌های انجام شده را به صورت یک رکورد یا سابقه الکترونیکی حفظ می‌کنند. این قابلیت در خدمات الکترونیکی، سرخ‌های پژوهشی بیشتری برای سازمان اجراکننده قوانین فراهم کرده و کمک شایانی به فرآیند پیگیری می‌نماید؛ به طور مثال در صورتی که احراز هویت مشتری انجام نشود (مانند مشتریانی که ناشناس باقی می‌مانند)، در برخی موارد یک سابقه الکترونیکی می‌تواند، حتی با حداقل داده موجود

۱. پول‌شویی نوین با استفاده از روش‌های نوین پرداخت. (۲۰۱۰).

2. FATF, Ibid. (2010).

از قبیل IP Address یا مکانی که پرداخت یا برداشت وجوه صورت گرفته، فرآیند پیگیری و اجرای قانون را بهبود بخشد؛<sup>۱</sup> این قابلیت می‌تواند به‌طور بالقوه، محل یا هویت کاربر مشکوک به پول‌شویی و تأمین مالی تروریسم را شناسایی نماید.<sup>۲</sup>

بنابراین، رعایت قوانین و الزامات مپ/تت از سوی ارائه‌دهنده‌گان خدمات الکترونیکی، به شفافیت بیشتری در تراکنش‌ها منجر می‌شود. همچنین، خدمات الکترونیکی (با توجه به پتانسیل جذب مشتریان بیشتر) می‌تواند، مشتریان را از بخش‌های بدون نظارت و یا حتی غیرقانونی بازار خدمات (مانند حواله‌ها یا خدمات بانک‌های زیرزمینی)، به سمت بازارهای رسمی سوق دهد.

### ۳-۲. ارزیابی ارائه‌دهندگان خدمات

یکی از یافته‌های گزارش سال ۲۰۰۶ سازمان FATF این موضوع بود که ریسک‌ها و آسیب‌پذیری‌های پول‌شویی و تأمین مالی تروریسم میان ارائه‌دهندگان خدمات و محصولاتشان حتی بین یک گروه یکسانی از خدمات نوین پرداخت، مانند کارت‌های اعتباری به‌طور قابل توجهی متفاوت هستند. مسأله یادشده به این واقعیت اشاره دارد که محصولات مختلف ویژگی‌های مختلفی دارند (ارائه‌دهندگان متفاوتی آنها را ارائه می‌دهند) که روی مشخصات ریسکی آنها تأثیر می‌گذارد.

### ۳-۳. ماتریس ریسکی

برخی از عوامل ریسکی به‌طور مستقیم نتیجه نوع خدمات است (از قبیل ناشناس ماندن، روش‌های تأمین مالی و محدودیت مقادیر)، در حالی که بقیه، نتیجه اقدامات ارائه‌دهندگان خدمات (از قبیل احراز هویت و روش‌های کنترلی) هستند.

۱. برای مثال، ممکن است مجریان قانون قادر به ارائه تصویر یک مظنون با استفاده از CCTV (دوربین‌های مدار بسته) باشند و این اطلاعات می‌تواند با استفاده از اطلاعات جغرافیایی مکانی که خدمات مورد استفاده قرار گرفتند (مانند ATMها و کافی‌نت‌ها) به دست آید.

۲. منتقدان، فواید آثار الکترونیکی ارائه‌شده توسط خدمات یا محصولات بدون شناسایی را به چالش کشیده و به این نکته اشاره می‌کنند که ممکن است آدرس IPها جعلی باشند؛ یا ممکن است مربوط به مراکز عمومی از قبیل "Hot Spots" یا کافه‌های اینترنتی باشند. در چنین مواردی، اطلاعات قابل استفاده کمی برای مجریان قانون وجود دارد، به‌ویژه در کشورهایی که نظارت‌های تصویری عمومی و خصوصی مانند دوربین‌های مدار بسته استفاده کمتری دارد.

در ماتریس زیر، عوامل مؤثر در میزان ریسک محصولات در چارچوبی استاندارد طراحی شده است که بر اساس شرایط داخلی و منطبق با استاندارد سازمان FATF است. باید به این نکته توجه داشت که به عوامل ریسکی عنوان شده در ماتریس زیر نباید به صورت موردی نگاه شود؛ بلکه باید به صورت کلی مدنظر قرار گیرد؛ دادن رتبه "ریسک بالا" برای یک عامل ریسکی لزوماً به معنی رتبه کلی این محصول به عنوان محصولی با ریسک بالا نیست. مهم، داشتن نگاه کلی است و این دید کلی نه تنها شامل تمام عوامل ریسکی می‌شود، بلکه تمامی تعدیل‌دهنده‌های ریسکی را نیز در بر می‌گیرد.<sup>۱</sup>

جدول ۱. عوامل ریسکی در خدمات نوین الکترونیکی

معیارها/ضوابط		روش‌های ریسک بالا	روش‌های ریسک پایین
۱	CDD / شناسایی مشتری	بدون شناسایی	شناسایی شده است
	احراز هویت	شناسایی شده اما احراز هویت نشده است	شناسایی و احراز هویت شده است.
	نظارت	عدم نظارت	وجود نظارت مستمر بر روابط تجاری
۲	ثابت سوابق / ثبت اسناد		سوابق تراکنش‌های الکترونیکی نگهداری می‌شوند، اما ثبت یا دسترسی مطلوبی وجود ندارد.
۳	محدودیت مقادیر	حداکثر مقادار موجودی حساب‌های هر شخص	دارای محدودیت
		حداکثر مقدار در هر تراکنش (مانند برداشت)	بدون محدودیت
		حداکثر تعداد تراکنش	دارای محدودیت در تراکنش‌ها
۴	محدودیت‌های کاربردی	نقدشوندگی (مقبولیت در تجارت)	مورد پذیرش گروه وسیعی از مردم از جمله تجار و بازرگانان ابزار معاملاتی با مقبولیت بالا (مانند ویزا <sup>۲</sup> و مستر کارت <sup>۳</sup> استاندارد)
		کاربردپذیری	امکان استفاده آنلاین از محصول، مثال: کاربرد آنلاین برای

1. FATF, Ibid. (2010).

2. VISA

3. MasterCard

روش‌های ریسک پایین	روش‌های ریسک بالا	معیارها/ضوابط	
تراکنش‌های P۲b، b۲b. ممکن باشد اما p۲p، ممکن نباشد.	انتقال وجه بین مشتریان یک بانک، از جمله P۲b (تراکنش میان شخص با شرکت)، b۲b <sup>۲</sup> (شرکت با شرکت)، p۲p <sup>۳</sup> (شخص با شخص)		
گزینه‌های برداشت/ انتقال محدود. مانند حساب‌های ارجاع داده شده؛ مقدار و تعداد برداشت محدود (مانند مبلغ ثابت معینی برای هر سال)	برداشت/ انتقال نامشخص و نامحدود (مانند پول نقد از طریق ATMها)	برداشت / انتقال	
تمام تراکنش‌ها بوسیله یک ارائه‌دهنده‌ی خدمت مرکزی، انجام می‌گیرد	تعدادی از ارائه دهندگان خدمات مستقل از هم، مراحل خاصی از تراکنش‌ها را بدون نظارت و هماهنگی مؤثر به صورت جداگانه انجام می‌دهند	تعامل متقابل ارائه‌دهندگان خدمات	
تمام فرآیندها به طور متمرکز تحت یک استاندارد سطح بالا، کامل می‌شود.	تعدادی از مراحل خاص برون‌سپاری می‌شوند؛ برون‌سپاری به دیگر مراجع قضایی بدون تدابیر امنیتی - حفاظتی خاص؛ عدم نظارت و وجود خطوط مسئولیت‌پذیری مشخص	برون‌سپاری	۵ تقسیم‌بندی خدمات

### ۳-۴. شناسایی کامل مشتری

بر اساس قوانین بانک مرکزی ایران، ارائه خدمات غیرپایه و پایه، منوط به شناسایی اولیه و کامل مشتریان<sup>۴</sup> است. بدین ترتیب، کاربران خدمات الکترونیکی از جمله خدمات اینترنتی، تلفن‌بانک و همراه بانک باید مشتری بانک باشند تا بتوانند از این گروه خدمات بهره‌مند شوند. در این خصوص با توجه به اینکه تمام مشتریان بانک در زمان افتتاح حساب، شناسایی و احراز هویت می‌شوند، در صورت شناسایی مناسب در زمان تعریف مشتری و افتتاح حساب، ریسک کمی شامل حال بانک‌ها خواهد بود. بنابراین، بانک‌ها باید در بخش شناسایی و احراز هویت، دقت لازم را مبذول نمایند تا مشتریان با ریسک بالا مشمول محدودیت‌های خاص و نظارت مستمر بر عملکردشان باشند. باید به این موضوع نیز توجه شود

1. Person to Business
2. Business to Business
3. Person to Person

۴. دستورالعمل چگونگی شناسایی مشتریان ایرانی مؤسسات اعتباری.



که اگر شناسایی مناسبی در هنگام تعریف مشتری و افتتاح حساب مشتریان صورت نگرفته باشد و یا در ثبت تراکنش‌های اینترنتی مشکل و یا شکافی وجود داشته باشد، ریسک پول‌شویی با توجه به میزان مشکلات و نواقص موجود، بالا خواهد رفت.

### ۳-۵. ثبت اطلاعات

در مورد ثبت اطلاعات و با توجه به پایگاه داده اطلاعات موجود در هر بانک، باید بررسی شود که آیا تمامی تراکنش‌های مالی و غیرمالی اینترنتی با تمامی اطلاعات جانبی شامل زمان، کاربر انجام‌دهنده، نوع تراکنش و جزاینها در پایگاه اطلاعاتی ویژه‌ای ثبت می‌شود یا خیر. همچنین، دسترسی به اطلاعات ثبت شده و تعبیه مسیر یا مسیرهای به منظور استخراج گزارش‌هایی کاربردی، اهمیت به‌سزایی در امر کنترل و نظارت دارد. نبود دسترسی راحت و سریع، فرآیند نظارتی و کنترلی را با مشکلات ناکارایی پایگاه اطلاعاتی مورد نظر مواجه کرده و در عمل، پایگاه اطلاعاتی، کارایی خود در تسهیل استخراج گزارش‌های تحلیلی را از دست می‌دهد. باید توجه داشت، گسترش روزافزون خدمات اینترنتی امکان نبود داده‌ها و یا نبود ذخیره اطلاعات لازم و جانبی به‌صورت کامل و دقیق در برخی موارد ریسک بالایی را به بانک‌ها تحمیل کرده است. به همین دلیل، وجود سیاست ویژه‌ای در خصوص ثبت اطلاعات، در هر بانکی امری ضروری است.

### ۳-۶. محدودیت مقادیر

اصطلاح "محدودیت مقادیر" به مواردی مانند موجودی بیش از حد مجاز، برای یک حساب یا یک محصول، محدودیت در مقدار هر تراکنش یا محدودیت در تعداد یا مقدار تجمیعی تراکنش‌های مجاز در طول یک دوره مانند روز/هفته/ماه/سال یا ترکیبی از محدودیت‌های پیش‌گفته اشاره می‌کند. همچنین، مواردی مانند تعداد حساب یا کارت‌های مجاز برای هر شخص نیز می‌تواند به عنوان یک نوع "محدودیت مقادیر" در نظر گرفته شود.

در مناطقی که محدودیتی برای تراکنش‌ها و مقادیر اعمال نشده، محدوده سرمایه در دسترس همان مقدار کل موجودی حساب محسوب می‌شود. این امر باعث افزایش احتمال پول‌شویی و به دنبال آن ریسک پول‌شویی و تأمین مالی تروریسم می‌شود که محصولات با آن مواجهند. تراکنش‌های با میزان و/یا تعداد بالا، ریسک پول‌شویی و تأمین مالی تروریسم بیشتری دارند. به‌طور مشابه، انتخاب بازه‌های وسیع با محدودیت‌های اندک و یا نبود محدودیت روی حساب‌ها نیز به افزایش ریسک منجر می‌شود. اغلب ارائه‌دهندگان خدمات پرداخت سیار (موبایل) محدوده مقادیر نسبتاً کم (یعنی محدودیت شدیدی) را روی محصولاتشان اعمال می‌کنند. همچنین، برای خدمات اینترنتی یا خدمات کارت‌های اعتباری، طیف وسیعی از روش‌های ایجاد محدودیت وجود دارد. برای مثال، کارت‌های اعتباری شاید به عنوان یک کارت غیرقابل شارژ با سقف حساب نسبتاً کم طراحی شده باشند. از سوی دیگر، کارت‌های قابل شارژی بدون سقف یا با سقف بالا نیز وجود دارند که به نسبت ریسک بالاتری خواهند داشت.

ارائه‌دهندگان محصولات با حدود بالا یا بدون محدودیت، اغلب در حوزه‌های قضایی یا کشورهایی حضور دارند که در آن ارائه‌دهندگان خدمات این نوع خدمات از نظم و نظارت یکپارچه و مناسبی از منظر مپ/ت پیروی نمی‌کنند و یا سیستم بررسی و نظارتی مناسبی ندارند. این درحالی است که این افراد، محصولات خود را به‌صورت بین‌المللی می‌فروشند (از طریق نمایندگی‌ها یا اینترنت). بدین ترتیب، این‌گونه از ارائه‌دهندگان که خدماتی بدون حدود یا با حدود بالا ارائه می‌دهند، ممکن است در حوزه‌های قضایی با حاکمیت و نظارت مقرراتی قوی نیز یافت شوند.<sup>۱</sup> باید توجه داشت، عموماً ارائه کارت‌های ناشناس اغلب توسط خود شرکت صادرکننده انتشار داده نمی‌شود، بلکه توسط واسطه‌هایی که برخی از آنها تخصص فروش به شرکت‌های خارجی را دارند، ترجیحاً در مناطقی که پناهگاه‌های مالیاتی هستند، انتشار می‌یابند و در نتیجه آن، یک "بسته خصوصی" کاملی را به مشتریان خود ارائه می‌دهند.

۱. در سال ۲۰۰۷، Bundeskriminalamt آلمان (BKA) پژوهش ویژه‌ای روی کارت‌های پرداخت انجام داد. در این پژوهش، BKA شش نمونه از کارت‌های پرداخت ناشناس کشف کرد که از طریق اینترنت فروخته می‌شود. بانک‌های منتشرکننده در اروپا و آمریکای مرکزی واقع بودند.

شاید محدودیت مقادیر با شناسایی کامل مشتریان مرتبط باشد (یعنی محدودیت‌های سخت برای مواردی که میزان سطح شناسایی مشتریان پایین است و محدودیت‌های کم و یا بدون محدودیت برای مواردی که میزان سطح شناسایی مشتری بالا است).<sup>۱</sup>

بر اساس بخشنامه‌های نظام‌های پرداخت بانک مرکزی ایران، در داخل کشور نیز محدودیت مقادیر وجود دارد. در این راستا می‌توان به "دستورالعمل صدور دستور پرداخت و انتقال وجوه" اشاره کرد. در این دستورالعمل، تمامی انتقالات از انواع مسیرها (انتقال کارت به کارت از طریق اینترنت، پایانه‌های PINPAD یا POS و یا خودپردازها و جزاینها) ملزم به رعایت استانداردهای ویژه‌ای هستند که طبق این استاندارد جزئیات هر انتقال در یک دستور پرداخت باید به یکی از اشکال زیر تنظیم شود:

- مستمر محدود: ذکر هر یک از مبالغ انتقال و تاریخ‌های مؤثر آنها، به‌طوری‌که تعداد انتقالات محدود باشد. به‌عنوان مثال، پرداخت اقساط یا اجاره‌بهای دوازده ماهه در ابتدای هر ماه خورشیدی،
- نامعین (و مستمر) و محدود: ذکر تاریخ‌های مؤثر انتقالات قابل انجام، به‌طوری‌که تعداد انتقالات محدود باشد. به‌عنوان مثال، پرداخت حقوق و مزایای کارکنان در دوازده ماه آینده در پایان هر ماه خورشیدی،
- نامعین (و مستمر) و نامحدود: ذکر مقطع زمانی انتقالات قابل انجام، به‌طوری‌که تعداد انتقالات محدود نباشد. به‌عنوان مثال، پرداخت مبلغ قبوض برق در فاصله ده روز اول ماه‌های زوج خورشیدی تا اطلاع ثانوی.<sup>۲</sup>

گفتنی است، محدودیت مقادیر در انتقالات داخل هر بانک به نسبت محدودیت‌های وضع شده در تراکنش‌های بین بانکی از سخت‌گیری‌های کمتری برخوردار است؛ زیرا ریسک پ/ت در مواردی که در فرآیند انجام تراکنش، پای چندین مؤسسه در میان است، بیشتر خواهد بود. در صورتی که

1. FATF, Ibid. (2010). and Centre, Ibid. (2013).

۲. دستورالعمل صدور دستورپرداخت و انتقال وجوه.

تراکنش‌های داخل هر بانک قابلیت نظارت و پیگیری بسیار بالاتری دارند. از سوی دیگر، باید دقت شود محدودیت اعمال شده در ایران بیشتر حول محور مقدار وجوه متمرکز است و محدودیت در تعداد تراکنش‌ها کمتر مشاهده می‌شود.

از سوی دیگر در ایران، محدودیت در سقف انتقال وجوه از طریق مختلف، به دلیل تفاوت در سطح امنیت، قابلیت‌های پیگیری، دقیق بودن اطلاعات ثبت شده در پایگاه داده و جزاینها متفاوت هستند. مشخص است، تراکنش‌های انتقال از طریق شعبه که با نظارت مستقیم کاربر شعبه همراه است، با ریسک کمتری به نسبت تراکنش‌های انتقال از طریق تلفن همراه، خودپردازها و POSها روبه‌روست. بنابراین، به نظر می‌رسد، "محدودیت‌های مقادیر" موجود در سیستم بانکی داخل کشور در بیشتر موارد متناسب با سطح ریسک پ/ت آن است. هر چند تمامی محدودیت‌های اعمال شده در این حوزه، مربوط به مقدار انتقال در طول یک روز است و نسبت به سقف انتقال در هفته، ماه و یا سال اقدامات ویژه‌ای صورت نگرفته است. بنابراین، انتظار می‌رود با مطالعات بیشتر و پژوهش‌ها در انواع حساب‌های موجود و دسته‌های مختلف مشتریان، استاندارد ی با انعطاف بیشتر و با محدودیت‌های بهینه‌تری اعمال شود. در این راستا، تعیین سطح فعالیت مشتریان و محدود نمودن تراکنش‌ها با توجه به کمینه و بیشینه و یا متوسط فعالیت مشتریان، می‌تواند گام‌های بعدی در این بخش باشند.

### ۳-۷. محدودیت‌های کاربردی

محدودیت‌های کاربردی برای خدمات نوین بانکی می‌تواند از یک محصول به محصول دیگر متفاوت باشد. محصولات نوین با قابلیت کاربرد محدود، دارای ریسک پ/ت کمتری نسبت به خدماتی هستند که به مشتریان بازه وسیعی از کاربرد را ارائه می‌دهند.

کارت‌های اعتباری قابل شارژ به‌ویژه در مواردی که با استانداردهای مطلوب و بازه وسیعی انتشار می‌یابند (مانند ویزا و مستر کارت)، معمولاً کمترین محدودیت کاربردی را دارند، به طوری که متکی به وجود زیرساخت‌های گسترده برای تراکنش‌های پرداخت بوده و عضو شبکه ATM جهانی هستند و در نتیجه، قابلیت تبدیل به پول نقد و خرید و فروش را دارند.

### • نقدشوندگی

امروزه ویزا و مستر کارت، مورد پذیرش تجار داخلی و خارجی است. استانداردهای استفاده شده در ارائه این نوع کارت‌ها تا حد زیادی مشابه<sup>۱</sup> با کارت‌های بدهی و اعتباری است. همچنین، برخی از این کارت‌ها در تمامی جاهایی پذیرفته می‌شود که کارت‌های اعتباری مورد استفاده قرار می‌گیرند؛ مانند خریده‌های اینترنتی برخط.

در خصوص برخی خدمات مانند خدمات همراه بانک، تراکنش‌های پرداخت اغلب تنها در محدوده مشتریان مؤسسه ارائه‌دهنده آن خدمت (مانند یک بانک) امکان‌پذیر است؛ بنابراین، نقدشوندگی محدودتری نسبت به دسته پیشین خواهند داشت. از سوی دیگر، خدمات پرداختی که تراکنش‌های بین بانکی را از طریق همراه بانک امکان‌پذیر می‌کنند، معمولاً از مقبولیت بیشتری در میان پول‌شویان به نسبت مواردی که قابلیت‌های کمتر و محدودیت‌تری دارند، برخوردارند. در برخی موارد، خدمات همراه بانک به تراکنش‌های خرد مانند خرید یا شارژ کارت‌های سیستم‌های حمل و نقل، بلیط‌ها و کارت‌های دستگاه‌های فروش خودکار محدود می‌شوند که در این صورت، دارای محدودیت‌های کاربردی زیادی خواهند بود؛ اما ممکن است در برخی بازارهای دیگر (در حوزه‌های دیگر قضایی)، قابلیت نقدشوندگی بیشتری داشته و در نتیجه از منظر پ/ت ریسک بیشتری خواهند داشت.

### • کاربردپذیری

در کارت‌های نقدی قدیمی، استفاده از کارت‌ها منوط به در دسترس بودن برخی امکانات خاص بوده است (مانند دستگاه‌های کارت‌خوان و دسترسی برخط به سیستم). بنابراین، بیشتر دریافت‌کنندگان کارت‌های پرداخت، شرکت‌ها بوده‌اند (با قابلیت تراکنش پرداخت از شخص به شرکت). اگرچه پس از افزایش قابلیت‌های این نوع از کارت‌ها از جمله دریافت یا انتقال وجوه، پرداخت مبالغ از منابع خارجی

۱. کشورها یا مؤسسات می‌توانند راهکارهای کنترلی مختلفی به منظور پیشگیری از کاربرد کارت‌های نقدی فقط به منظور خرید یک کالا یا محصول خاص، برداشت از طریق دستگاه‌های ATM اتخاذ نمایند و یا مبلغ و میزان تراکنش‌ها را محدود نمایند. به همین دلیل، کاربرد کارت‌های نقدی می‌تواند بسیار متفاوت‌تر از کارت‌های اعتباری باشد.

و یا قابلیت انتقال به شخص سوم و حساب‌های دیگر، امکان پرداخت‌های شخص به شخص نیز به وجود آمده و کاربرد آن بیشتر شده است. بدین ترتیب، در خصوص کاربردپذیری سایر خدمات نیز می‌توان میزان خاصی از کاربردپذیری را تعریف کرده و آن را به عنوان یکی از عوامل ریسکی در محاسبات وارد کرد. بنابراین، به صورت کلی افزایش کاربرد یک نوع خدمت یا محصول با افزایش کنترل و نظارت همراه است تا ریسک سوء استفاده از آن در پ/ت مدیریت شود.

### • خروج وجوه

پول نقد می‌تواند از طریق کارت‌های نقدی با استفاده از شبکه خودپردازها از یک حساب خارج شود. افزون بر این، ممکن است در برخی کشورها دریافت وجوه نقد به وسیله خرید جنس و پرداخت مبلغ بیشتر از ارزش واقعی و دریافت نقدی مابقی مبلغ پرداخت شده، امری آسان و معمول باشد. این نوع خروج نقدینگی به "بازگشت نقدی" معروف است.<sup>۱</sup> دسترسی آسان به پول نقد و نقدشوندگی یا قابلیت معاملاتی بالا در کنار تسهیل کارت‌های نقدی با موجودی پیش‌پرداخت شده،<sup>۲</sup> ممکن است برای انتقال وجوه در مبالغ بالا جایگزین مناسبی برای پول نقد شود؛ به‌ویژه در طرح‌های قاچاق پول نقد با مبالغ بالا با فرض امکان ایجاد تعداد زیادی حساب و بدون احراز هویت، قابلیت خروج وجوه، ریسک بالایی را به مؤسسات ارائه‌دهنده آن خدمت تحمیل خواهد کرد.

انتقال از هر حساب به حساب دیگر در داخل هر بانک، خدمتی است که در تمام بانک‌های ایران ارائه می‌شود. در حالی که انتقال به حسابی نزد بانکی دیگر در اغلب بانک‌ها به صورت اینترنتی (پایا و یا ساتنا) ممکن است؛ اگر این انتقالات و تراکنش‌ها بدون هیچ محدودیت خاص یا نظارتی صورت پذیرد، احتمال استفاده پول‌شویان از این کانال‌ها افزایش خواهد یافت.

۱. روش "بازگشت نقدی" که یکی از روش‌های خروج جریان وجوه نقد بوده و در اصل، به منظور خروج پول نقد از کارت‌های اعتباری و بدهی توسعه یافته است و مورد استفاده قرار گرفت.

۲. کارتی که به عنوان یک وسیله برای خروج وجوه و یا پرداخت‌های ضروری استفاده می‌شود. مانند کارت‌های نقدی موجود در سیستم بانکی داخل ایران که تمام مبلغ موجود در کارت قبلاً پیش‌پرداخت شده است.

افزون بر تمام نکات مورد بحث در این بخش، کشورها باید اطمینان یابند، مؤسسات مالی، هنگام انجام فرآیند نقل و انتقالات الکترونیکی، طبق تعهدات مقرر در قطعنامه شورای امنیت سازمان ملل (شماره ۱۲۶۷ سال ۱۹۹۹ و شماره ۱۳۷۳ در سال ۲۰۰۱) در خصوص ممنوعیت و سرکوب تروریسم، دارایی‌های افراد و مؤسسات مظنون به فعالیت تروریستی را مسدود و انجام هرگونه معامله با اشخاص یادشده را ممنوع می‌کنند.<sup>۱</sup>

### ۳-۸. تقسیم‌بندی خدمات

در این بخش، موضوع مورد نظر به خدماتی برمی‌گردد که در آنها بخشی از مراحل خدمات‌رسانی، از سامانه‌های غیر از یک بانک خاص استفاده کرده و نیازمند همکاری چند سیستم و نهاد مختلف است؛ مانند انتقالات پایا و استفاده از درگاه اینترنتی بانکی دیگر، به منظور انتقال وجوه از طریق اینترنت. این موارد دارای ریسک بیشتری به نسبت مواردی هستند که تمامی تراکنش‌ها از سیستم‌های یک بانک خاص استفاده می‌نمایند.

### ۴. جمع‌بندی

#### ۴-۱. محاسبات ریسک پ/ت با استفاده از ماتریس ریسکی

یکی از متداول‌ترین و ساده‌ترین رویکرد استفاده از شاخص‌های ارائه‌شده در ماتریس ریسکی بخش ۳-۳ اختصاص امتیاز به هر دسته (کم ریسک و پر ریسک) است. پس از تجمیع امتیازات کل ماتریس، به‌منظور رتبه‌بندی سطح ریسک آن سعی می‌شود کل امتیازات مورد انتظار را به چندین دسته کلی با رتبه‌های به ظاهر ساده‌تر طبقه‌بندی نمود. بدین‌منظور، کل بازه امتیازات را به چندین دست تقسیم کرده و به هر دسته، رتبه‌ای اختصاص می‌دهیم. رتبه به‌دست‌آمده در این مرحله به عنوان رتبه ریسک پول‌شویی و تأمین مالی تروریسم محسوب می‌شود. به عنوان مثال، به موارد کم ریسک امتیاز ۵ و به موارد پر ریسک امتیاز ۱۰ اختصاص می‌دهیم. با توجه به اینکه ستون‌های پایانی ماتریس ریسکی مطرح‌شده در این پژوهش ۱۲ سطر دارد، به صورت کلی، تمامی خدمات و محصولات بانکی نمره‌ای

۱. کشتکار. (۱۳۹۳).

بین ۶۰ (در کم ریسک‌ترین حالت) تا ۱۲۰ (در پر ریسک‌ترین حالت) خواهند داشت. حال، همان‌طور که گفته شد، مرحله دسته‌بندی یا طبقه‌بندی را خواهیم داشت. در این مورد، به عنوان یک روش پیشنهادی، می‌توان امتیازات را به بازه‌هایی به طول ۲۰ واحد تقسیم کرد. در این صورت به بازه ۶۰-۸۰ رتبه ۳، بازه ۸۰-۱۰۰ رتبه ۲ و بازه نهایی نیز رتبه ۱ اختصاص می‌دهیم. بدین ترتیب، رتبه ۳ کم ریسک‌ترین و رتبه ۱ پرریسک‌ترین محصول تلقی می‌شوند.

روش تشریح شده در پاراگراف پیشین، یکی از ساده‌ترین روش‌ها بوده و تسهیل شده روش‌های استفاده شده در سیستم بانکی کشور پاکستان، استرالیا و برخی شرکت‌های رتبه‌بندی بین‌المللی است. باید متذکر شد که روش‌های محاسباتی با ورود میزان زیان مورد انتظار در هر طبقه، سطح ریسکی پیچیده‌تر و دقیق‌تر را ارائه خواهند داد. همچنین در بیشتر موارد سه طبقه به ترتیب، بدون ریسک، ریسک متوسط و با سطح ریسک بالا مطرح می‌شود و ماتریس ریسکی مطرح شده در این مقاله منطبق با این سه دسته توسعه می‌یابد.

لازمه ارائه محاسبات، مدل‌سازی‌ها و روش‌های رتبه‌بندی پیشرفته‌تر، تجمیع داده‌های زیان و مطالعات دقیق در طی زمان خواهد بود (معمولاً از داده‌های زیان تجمیع شده حداقل برای سه سال به منظور مدل‌سازی و محاسبه میزان زیان هر عامل ریسکی استفاده می‌شود). بنابراین، انتظار می‌رود، در هر حوزه قضایی، فرآیند کمی‌سازی ریسک پ/ت و رتبه‌بندی آن همانند ریسک‌های دیگر بانکی (شامل ریسک‌های اعتباری، عملیاتی، نقدینگی، بازار و جزاینها)، با مدل‌های اولیه و ابتدایی شروع شده و در فرآیند توسعه قرار گیرد.

در ادامه برای هر رتبه، سیاست‌های نظارتی و کنترلی مخصوصی تعریف و در عمل نیز اجرا می‌شود. این فرآیند به صورت دوره‌ای بازنگری شده و در برخی موارد اصلاح می‌شود تا بدین وسیله یک حوزه قضایی، شاخص‌های پول‌شویی و تأمین مالی تروریسم مطابق با ساختار قضایی خود را داشته باشد.



#### ۴-۲. اقدامات و کنترل‌ها برای موقعیت‌های پریسک

برای شناسایی بیشتر ریسک مشتری و ریسک‌های دیگر به سرمایه‌گذاری و صرف زمان مناسب نیاز است. بهتر است با توجه به پیشینه اجرایی کشورهای مختلف، مراحل و مراتب زیر در سیستم بانکی کشورمان نیز دنبال شود:<sup>۱</sup>

۱. آگاهی بیشتر مؤسسه از موقعیت‌های پریسک،
۲. شناسایی مشتری به صورت دقیق‌تر و کامل‌تر،
- دسته‌بندی مشتریان به سه گروه کم ریسک، ریسک متوسط و ریسک بالا به‌منظور پیاده‌سازی رویکرد مبتنی برریسک.
۳. بالا بردن سطح توافق‌ها حین افتتاح حساب و تعریف مشتری،
۴. نظارت بیشتر بر معاملات،
- دسته‌بندی معاملات،
- شناسایی فعالیت کسب و کار،<sup>۲</sup>
- میزان دارایی (پول) + تناوب معاملات.
۵. افزایش سطح کنترل‌های مستمر.

بدیهی است که باید مراحل بیشتری به این ساختار اضافه شود. این کار منوط به پژوهش‌های بیشتر و بومی‌سازی ساختارهای پیاده‌سازی شده در کشورهای دیگر و نیز مستلزم استفاده از تجارب داخلی بین‌المللی است.

همان‌طور که اشاره شد، در خصوص بررسی خدمات بانکی از منظر ریسک پول‌شویی و تأمین مالی تروریسم، کارهای مشابهی در کشورهای دیگر صورت گرفته است؛ اما به دلیل ماهیت فعالیت‌های پول‌شویی - که کاملاً مرتبط به بستر موجود در هر جامعه بوده و در حوزه‌های قضایی مختلف متفاوت است - نتیجه به‌دست آمده برای هر کشور متفاوت از کشور دیگر خواهد بود. در این راستا، می‌توان با

1. Central Bank of Nigeria, Ibid. (2011). and Price, Ibid. (2008). and The Information Policy Team, Ibid (2012).

2. Business Activity

بررسی پرونده‌های موجود در هر حوزه قضایی، شاخص‌های ویژه همان حوزه قضایی را استخراج و الگوریتم متناسب برای محاسبه ریسک پول‌شویی و تأمین مالی تروریسم ارائه داد.



## منابع

- ارجمندنژاد، عبدالمهدی و کاظمیان، مهدی. (۱۳۹۲). مجموعه قانون و مقررات مبارزه با پول شویی اداره مبارزه با پول شویی تهران. بانک مرکزی.
- بیابانی، غلامحسین و عصار، محمد تقی. (خرداد و تیر ۱۳۸۸). پول شویی، خطری برای امنیت اقتصادی و اجتماعی. شماره‌های ۲۶۲ و ۲۶۱.
- پاکروان، لقمان. (تابستان ۱۳۸۹). گذری بر فرآیند پول شویی و آثار آن در بخش‌های اقتصادی. حسابرس. ۴۹.
- تذهیبی، فریده. (۱۳۸۹). پول شویی و روش‌های مبارزه با آن. تهران. انتشارات جنگل. کمیته ایرانی اتاق بازرگانی بین‌المللی.
- کشتکار، مریم. (۱۳۹۳). رویکرد و نظارت مبتنی بر ریسک برای پیشگیری از پول شویی و تأمین مالی تروریسم. مدیریت کل مقررات، مجوزهای بانکی و مبارزه با پول شویی اداره مبارزه با پول شویی. تهران، بانک مرکزی.
- مهجوریان، فریده. (۱۳۹۲). جزوه آموزشی دوره تربیت مدرس مبارزه با پول شویی و تأمین مالی تروریسم. جزوه کلیات پول شویی و مبارزه با آن. تهران، پژوهشکده پولی و بانکی بانک مرکزی.
- Australian Government. (2006). A Tool for Small-to-Medium Sized Businesses. Australian Transaction Reports and Analysis Centre.
- Central Bank of Nigeria. (2011). Central and Bank of Nigeria s Anit-Money Laundering/. Central Bank of Nigeria.
- Centre, D. I. (2013). Elements of a Risk Based AML Framework. Dubai: Total Solutions Middle East Limited.
- FATF. (2010). Money Laundering Using New Payment Methods. FATF.
- Price, C. (2008). Customer Risk Assessment.
- SAS Institute. (2009). Dynamic Risk Classification For Anti- Money Laundering.

- State Bank of Pakistan. (2012). AML/CFT Guidelines on Risk Based Approach for Banks and DFIs. Banking Policy and Regulations Department.
- The Information Policy Team, T. N. (2012). Anti-Money Laundering and Counter Terrorist Finance Report 2011-12. London: The National Archives.

