# روش‌های نوین پول‌شویی با رویکرد تبادلات مالی در فضای سایبری

مرجان بشخور[1]

به طور کلی پولشویی، یعنی مشروع جلوه‌دادن پول‌هایی که از راه‌های غیرقانونی و نامشروع به‌دست می‌آیند. در نوع سایبری پول شویی، از اینترنت و سایر بسترها و ابزارهای فضای مجازی برای مخفی کردن یا قانونی جلوه دادن پول حاصل از روش‌های نامشروع، استفاده می‌گردد. از جمله متداول‌ترین ابزارها و مکانیزم‌های مورد استفاده آنها می‌توان به مواردی مانند استفاده از حساب‌هایی که با کمک اسناد مفقودشده یا صاحبان غیرواقعی افتتاح شده‌اند، استفاده از شرکت‌های جعلی، استفاده از دسترسی از راه دور برای اجرای معاملات مالی از طریق حساب‌های بانکی متعدد، استفاده از پرداخت الکترونیک، خرید پول الکترونیکی و استفاده از کیف پول الکترونیکی و... اشاره کرد. در راستای کاهش تبعات شیوه نوین پولشویی بر امنیت اقتصادی کشور، در زمینه اتخاذ سیاست‌های ضد پول‌شویی از جمله ابعادی که باید مورد توجه قرار گیرند عبارتند از: شناسایی معاملات مالی مشکوک به پول‌شویی سایبری، حمایت قانونی برای جلوگیری و مقابله با قانونی کردن عواید جرایم سایبری و....

**کلیدواژه:** پولشویی، جرایم سایبری، معاملات مجازی، بانکداری الکترونیک.

در ادبیات اقتصادی به تمام عواید و درآمدهای ناشی از فعالیت‌های غیرقانونی پول کثیف[2] و به فرآیند وارد شدن این درآمدها به چرخه اقتصاد و حذف مبدأ تحصیل مال، پول‌شویی[3] گفته می‌شود. این پدیده نه‌تنها بر اقتصاد کشورها، بلکه بر روابط اجتماعی و سیاسی آنها نیز تأثیر منفی دارد. ازاین‌رو، کشورهای توسعه‌یافته با آگاهی از آثار منفی پول‌شویی، به تدوین قوانین و مقررات و اتخاذ تدابیر مؤثر برای مبارزه همه‌جانبه با آن پرداخته و در زمینه کنترل این جرم در چهارچوب نظام مالی خود موفقیت‌هایی به‌دست آورده‌اند. این در حالی است که کشورهای درحال‌توسعه- از جمله ایران- به دلیل وجود سازوکارهای نظارتی ضعیف در بازارهای مالی و عدم تأثیرگذاری کافی اقدام‌ها برای مبارزه با این جرم، به بستری مناسب برای شست‌وشوی عواید حاصل از فعالیت‌های مجرمانه تبدیل شده‌اند.

به‌طور کلی، نگاهی به آمارها و شاخص‌های پول‌شویی در ایران حاکی از آن است که از یک سو، به دلیل موقعیت جغرافیایی و از سوی دیگر، به دلیل شرایط نامساعد سیاسی- اقتصادی، ایران می‌تواند به

۱- پژوهشگر گروه اقتصاد مقاومتی و برآورد اقتصادی، مرکز پژوهشی امنیت اقتصادی تدبیر، تهران، ایران mballameh1398@gmail.com

2- Dirty Money

3- Money Laundering

بستری بالقوه برای فعالیت‌های پول‌شویی تبدیل شود. براساس آمارهای بین‌المللی، ایران در سال‌های ۲۰۱۵، ۲۰۱۶ و ۲۰۱۷ چه از نظر ناکارآیی سیاست‌های ضد پول‌شویی[1] (AML) و چه از نظر ریسک فعالیت‌های پول‌شویی (با نمره ریسک حدود ۸/۶) در جایگاه نخست بین کشورهای مورد بررسی قرار داشته است[2]. همچنین براساس آمارهای غیررسمی، حجم پول کثیف در چرخه اقتصاد کشور ۱۱/۸ درصد نقدینگی برآورد شده[3] و در نه‌ماهه نخست سال ۱۳۹۸، پرونده‌های پول‌شویی در کشور ۲۶۸ درصد رشد ریالی داشته است[4].

بنابراین، به نظر می‌رسد با توجه به بی‌ثباتی‌های مالی و اقتصادی در فضای کلان کشور و آثار منفی گسترش پدیده پول‌شویی در فضای اقتصادی- که می‌تواند در قالب کاهش سطح فعالیت‌های مولد، بیکاری و متعاقب آن افزایش جرم و جنایت، کاهش امنیت اجتماعی و افزایش هزینه‌های مبارزه با جرایم، گسترش انواع فسادهای مالی و اداری، افزایش فرار سرمایه و کاهش سرمایه‌گذاری‌های مولد، افزایش فاصله طبقاتی و تنزل پایگاه اجتماعی حکومت‌ها نمود یابد- باید ابعاد این پدیده مورد واکاوی بیشتر قرار گیرد. در همین چهارچوب، در این گزارش به بررسی روش‌های پول‌شویی در فضای مجازی، به‌عنوان یکی از اشکال متداول پول‌شویی در سال‌های اخیر، پرداخته می‌شود. بدین منظور، بخش دوم، به بررسی روش‌های اقدام به پول‌شویی در فضای مجازی، بخش سوم، به بیان ملاحظات امنیت اقتصادی این پدیده و در نهایت، بخش آخر، به بیان برخی راهکارهای پیشنهادی اختصاص دارد.

## ۱- روش‌های پول‌شویی در فضای مجازی

به‌طور کلی پول‌شویی سایبری مجموعه عملیات پول‌شویی است که از طریق سیستم‌های پرداخت شبکه‌ای از جمله شبکه‌های اینترنتی، محلی، ماهواره‌ای یا پرداخت وجوه از طریق تلفن همراه انجام می‌شوند. در این روش پول‌شویی، برخلاف روش‌های سنتی که بر نظام بانکی تکیه دارند، از انواع مختلف قراردادها و ارایه‌دهندگان خدمات مالی- که دامنه‌ای از انتقالات الکترونیکی، سپرده‌گذاری و برداشت نقدی، معاملات پول الکترونیکی و همچنین به‌کارگیری واسطه‌های انتقال‌دهنده پول[5] و خدمات حواله را دربر می‌گیرند- استفاده می‌شود.

در روش سنتی پول‌شویی، به‌طور معمول زنجیره پول‌شویی به دنبال معامله نقدی با استفاده از سیستم‌های پرداخت سنتی توسط واسطه‌های انتقال‌دهنده پول شکسته (شناسایی) می‌شود، اما اگر سیستم پرداخت انتخاب شده برای انجام عملیات پول‌شویی از قابلیت پرداخت آنلاین یکپارچه برخوردار باشد، پول غیرقانونی ابتدا به پول نقد الکترونیکی تبدیل و بدین‌ترتیب، امکان انتقال سریع و تقریباً ناشناس آن به خارج از کشور فراهم می‌شود. در این شرایط، شناسایی و ردیابی وجوه غیرقانونی توسط پلیس یا نرم‌افزارهای سنتی ضد پول‌شویی جمع‌آوری‌کننده داده‌ها براساس

1- Anti-Money Laundering *(AML)*

۱- از سال ۲۰۱۷ به بعد این شاخص برای ایران برآورد نشده است.

۲- خبرگزاری دنیای اقتصاد، کد خبر: ۳۴۱۳۲۸۱.

۳- خبرگزاری ایلنا، کد خبر: ۸۶۲۵۶۹.

4- Money Mules

الگوهای رفتار مشتری با چالش مواجه می‌شود. به‌علاوه، پلیس با چالش دیگری در این زمینه مواجه بوده و آن، خلأ موجود در ارتباط با ردیابی پول‌شویی از طریق سیستم‌های پرداخت آنلاین با قابلیت انجام معامله از راه دور است (گروه مبارزه با پول‌شویی و تأمین مالی تروریسم اوراسیا[1]، ۲۰۱٤).

به‌منظور شست‌وشوی عواید حاصل از جرم، مجرمان باید بسیار سریع و بدون باقی گذاشتن ردی از خود عمل کنند، به همین دلیل، بیشتر سازمان‌دهندگان و مجرمان پول‌شویی سایبری افرادی دارای صلاحیت فنی بالا و آموزش‌دیده هستند و بنابراین، روش‌های پول‌شویی ابداع شده توسط این افراد بسیار پیچیده و غیرمتعارف است. از جمله متداول‌ترین ابزارها و سازوکارهای مورد استفاده آنها عبارت‌اند از:

- استفاده از حساب‌هایی که با کمک اسناد مفقودشده یا صاحبان غیرواقعی افتتاح شده‌اند.
- استفاده از شرکت‌های جعلی (از جمله شرکت‌های جعلی حمل‌ونقل).
- استفاده از دسترسی از راه دور برای اجرای معاملات مالی از طریق حساب‌های بانکی متعدد.
- استفاده از پول نقد در مرحله نهایی زنجیره معاملات مالی.
- استفاده از سیستم‌های پرداخت جایگزین (مانند پرداخت الکترونیک) داخلی و بین‌المللی.
- خرید پول الکترونیکی و استفاده از کیف پول الکترونیکی.
- تبدیل عواید غیرقانونی به کالاها از طریق خرید کالاهای دست دوم از طریق اینترنت.
- خرید کالاهای آماده فروش یا کارت‌های پیش‌پرداخت و سپس، تبدیل (فروش) آنها به پول نقد.
- خرید بلیت‌ها، اسناد سفر (مانند گذرنامه، روادید، کارت گذرنامه و...)، وسایل خانه و... از طریق اینترنت و به‌منظور فروش مجدد.
- گرفتن اعتبار از خارج از کشور از طریق کازینو، قمارهای مجازی، فروشگاه‌های آنلاین و...

بررسی جرایم صورت گرفته در حوزه پول‌شویی سایبری حاکی از آن است که تبدیل وجوه غیرقانونی به پول نقد در آخرین مرحله پول‌شویی، از متداول‌ترین رویکردهای مجرمان حوزه پول‌شویی است، زیرا ردیابی پول نقد در خارج از نظام بانکی تقریباً غیرممکن است. براساس این، ابزارها و روش‌های مورد استفاده برای پیشگیری از این نوع پول‌شویی باید به‌گونه‌ای طراحی شود که تا پیش از مرحله آخر، جرم شناسایی شود. در این مرحله به‌طور عمده واسطهای انتقال‌دهنده پول به برداشت پول از دستگاه‌های خودپرداز و انتقال این وجوه به سازمان‌دهندگان جرایم سایبری اقدام می‌کنند. به‌علاوه، باید توجه کرد که برخی از این عواید غیرقانونی شسته‌شده به‌منظور خرید تجهیزات جدید و طراحی نرم‌افزارهای مخرب‌تر به‌منظور دور زدن سیستم‌های امنیتی سرمایه‌گذاری می‌شوند (گروه مبارزه با پول‌شویی و تأمین مالی تروریسم اوراسیا، ۲۰۱٤).

**۱-۲- استفاده از سیستم پرداخت جایگزین و پول الکترونیکی برای پول‌شویی**

استفاده از سیستم‌های پول الکترونیکی این امکان را برای مجرم فراهم می‌آورد که با سرعت و بدون

1-Eurasian Group on Combating Money Laundering and Financing of Terrorism

هیچ تلاشی منبع عواید حاصل از جرایم را در فضای سایبری از بین ببرد و این عواید را بشوید. در فرآیند انتقال الکترونیکی نیز ناشناس بودن در باز کردن و شارژ مجدد کیف پول الکترونیکی، دسترسی شبانه‌روزی و سرعت معاملات موجب استفاده گسترده مجرمان از این ابزار برای پول‌شویی شده است. نحوه عمل این نوع سیستم بدین‌گونه است که به‌منظور تبدیل شدن به کاربر سیستم پرداخت، فرد باید ثبت‌نام و یک حساب (کیف پول) الکترونیک باز کند که در آن اطلاعات مربوط به وجوه و معاملات کاربران در سیستم الکترونیک ذخیره می‌شود. معاملات مالی با استفاده از وجوهی که قبلاً کاربر در کیف پول الکترونیکی خود بارگذاری کرده است، انجام می‌شود. در سیستم‌های پرداخت مختلف به‌منظور اضافه کردن پول به کیف پول الکترونیکی از روش‌های مختلفی- از جمله: انتقال از طریق سیم، سفارش‌های پستی، کارت‌های پیش‌پرداخت، پایانه‌های پرداخت و...- استفاده می‌شود. سیستم‌های پرداخت الکترونیک با استفاده از پول الکترونیک عمل می‌کنند، یعنی یک ابزار مالی که به کاربر اجازه می‌دهد تا حق مطالبه را با استفاده از حساب‌های مجازی و سوابق الکترونیکی (ایمیل و...) مبادله یا به پول نقد و ابزارهای با نقدینگی بالای دیگر تبدیل کند. پول الکترونیک می‌تواند به‌منظور انجام معاملات مختلفی مورد استفاده قرار گیرد که از آن جمله آنها عبارت‌اند از:

- پرداخت‌های درون سیستمی به حساب‌های فردی و نهادهای قانونی.
- خریدهای آنلاین.
- پرداخت قبض‌های تلفن همراه، آب و برق.
- پرداخت برای دسترسی به اینترنت.
- پرداخت مالیات‌ها، عوارض و جرایم دولتی.
- خرید بلیت‌های هواپیما و قطار.
- خرید سوخت.
- رزرو هتل و...

در مجموع، می‌توان گفت، پول‌شویی در فضای سایبری نسبت به روش سنتی آن، مزایایی دارد که آگاهی از آنها می‌تواند در اتخاذ تدابیر لازم برای مبارزه با این جرم مؤثر باشد، برخی از مهم‌ترین آنها عبارت‌اند از:

➢ این روش پول‌شویی می‌تواند سبب افزایش سرعت در انجام مراحل سه‌گانه پول‌شویی[1] و تطهیر

---

۱- مراحل جرم پول‌شویی عبارت‌اند از:

- **جای‌گذاری:** نخستین مرحله جای‌گذاری یا تزریق عواید از فعالیت‌های مجرمانه به شبکه مالی رسمی با هدف تبدیل عواید از حالت نقدی به ابزارها و دارایی‌های مالی است. یکی از فن‌های جای‌گذاری اسمورفینگ است. در نخستین مرحله پول‌شویی همچنین می‌توان از تعاونی ساختمان‌سازی، شرکت‌های بیمه، باشگاه‌های خصوصی، کازینوها، رستوران‌ها و... نیز استفاده کرد.
- **لایه‌چینی:** لایه‌چینی به معنای تبدیل و جابه‌جایی پول از مکانی به مکان دیگر به‌منظور تغییر چهره دادن منشأ غیرقانونی وجه است، یعنی جداسازی عواید حاصل از جرم از منشأ غیرقانونی آن که از طریق ایجاد لایه‌های پیچیده مبتنی- بر معاملات (نقل‌وانتقال) و با هدف مبهم‌سازی زنجیره عطف حسابرسی، مجهول گذاشتن هویت طرف‌های اصلی معامله و عدم امکان ردیابی منشأ مال صورت می‌گیرد. این موضوع متضمن انجام عملیاتی مانند حواله وجه سپرده شده نزد بانک‌ها و مؤسسه‌های مالی به بانک‌ها و مؤسسه‌های دیگر یا تبدیل سپرده نقدی به اسناد پولی دیگر (اوراق بهادار ، سهام و چک‌های مسافرتی) است. یکی از فن‌های لایه‌گذاری اختلاط

اموال نامشروع شود و پول‌شویان با صرف هزینه کمتر به بالاترین منفعت مالی برسند.

- استفاده از تراکنش‌های الکترونیکی در فضای مجازی، باعث گمنامی و اختفای هویت پول‌شویان می‌شود.
- جرم پول‌شویی می‌تواند در فضای جغرافیایی گسترده‌تری در سطح ملی و جهانی انجام گیرد.
- کاهش حضور فیزیکی افراد در شعب و انجام نقل‌وانتقالات پولی به صورت الکترونیکی، می‌تواند باعث کاهش نسبی جرایمی مانند جعل اسناد به‌منظور مخفی نگه‌داشتن هویت و دادن رشوه به افراد توسط پول‌شویان در مؤسسه‌های مالی و بانکی شود.
- استفاده از فضای مجازی در بانک‌داری الکترونیکی و کاهش حضور فیزیکی افراد در شعب می‌تواند موجب کاهش ریسک خطر شناسایی مجرمان در مراحل پول‌شویی شود.

**بررسی جرایم صورت گرفته در حوزه پول‌شویی سایبری حاکی از آن است که تبدیل وجوه غیرقانونی به پول نقد در آخرین مرحله پول‌شویی، از متداول‌ترین رویکردهای مجرمان حوزه پول‌شویی است، زیرا ردیابی پول نقد در خارج از نظام بانکی تقریباً غیرممکن است.**

## ۱- ملاحظات امنیت اقتصادی

پیشرفت‌های تکنولوژیکی (فناورانه) گرچه در ابتدا به‌منظور افزایش رفاه بشر مورد بهره‌برداری قرار گرفتند، اما به‌تدریج به ابزاری برای مجرمان، به‌منظور نیل به آمال مجرمانه تبدیل شدند، به‌طوری که به‌موازات گسترش فعالیت‌ها و ارتباطات در فضای سایبری، بخشی از بزهکاران، به‌خصوص مجرمان پول‌شویی فعالیت مجرمانه خود را به این فضا منتقل کرده یا از طریق چنین فضایی مرتکب جرم شده‌اند. در ارتباط با جرم پول‌شویی در فضای سایبری- همان‌طور که در قسمت قبل اشاره شد، با توجه به سهولت انتقال عواید مجرمانه از طریق سیستم‌های الکترونیکی پرداخت و امکان استفاده از این عواید در حوزه‌های مختلف- این جرم می‌تواند آثاری منفی بر متغیرهای اقتصادی داشته باشد. باید توجه کرد، این پول‌ها به‌مثابه پول‌های بادآورده‌ای هستند که بدون خلق ارزش وارد چرخه درآمدی شده‌اند. از جمله این آثار اقتصادی- که می‌توانند در صورت کنترل نشدن جرم پول‌شویی سایبری به تهدیدی برای امنیت اقتصادی تبدیل شوند- عبارت‌اند از:

- **تبعات اقتصادی:** برخی از پیامدهای اقتصادی این جرم عبارت‌اند از: اختلال در چرخه درآمدی و تولید و در نتیجه، بروز یا تقویت رکود یا تورم، کاهش

---

پول کثیف با پول تمیز است؛ برای مثال، عواید حاصل از جرم با انجام معاملاتی مانند صادرات و واردات کالا و توسل به کم‌نمایی سیاهه صادراتی و گران‌نمایی سیاهه وارداتی وارد چرخه رسمی اقتصاد می‌شود.

- **یکپارچه‌سازی:** منظور از یکپارچه‌سازی فراهم کردن پوشش ظاهری مشروع و توجیه قانونی (قالبی مشروع) برای عواید حاصل از فعالیت‌های مجرمانه است. چنانچه مرحله لایه‌چینی با موفقیت انجام شود، عواید شسته‌شده با استفاده از طرح‌های یکپارچه‌سازی، به‌نحوی وارد جریان اصلی اقتصادی می‌شود که در بازگشت به نظام مالی، وجوه شکل و ظاهری قانونی یافته است. این مرحله ممکن است با استفاده از روش‌های متعددی مانند استفاده از شرکت‌های پوششی اعطای وام یا سپرده‌گذاری در مؤسسه‌های خارجی به‌عنوان وثیقه تأمین برای وام‌های داخلی، صورت پذیرد.

اعتماد به فضای سایبری برای انجام معاملات مالی، کاهش امکان فعالیت کسب‌وکارهای فین تک و توکنایز به دلیل قانون‌گذاری‌های غیرمؤثر و ناکارآ و از بین بردن زمینه‌های شکل‌گیری کسب‌وکارهای جدید همپای تحولات جهانی، اختلال در جمع‌آوری مالیات و تشویق فرار مالیاتی، اختلال در بازارهای مالی، افزایش نرخ تورم و انحرافات اجتماعی، رقابت‌پذیری ناسالم اقتصادی که موجب تضعیف بخش خصوصی و تعاونی می‌شود، تخریب بازارهای مالی، فرار سرمایه به صورت غیرقانونی، مال‌اندوزی مجرمان و کاهش بهره‌وری در بخش واقعی اقتصاد.

- **تبعات اجتماعی و بین‌المللی:** علاوه بر آثار مخرب اقتصادی، پول‌شویی خطرات و هزینه‌های اجتماعی زیادی نیز در پی دارد. این پدیده، امکان گسترش فعالیت‌های غیرقانونی را برای قاچاقچیان مواد مخدر، کالا، ارز و مجرمان دیگر فراهم می‌کند. همچنین شهرت یک کشور به پول‌شویی و تأمین مالی تروریسم و امنیت آن برای مجرمان، مانع توسعه آن کشور خواهد شد، ضمن آنکه انجام مبادلات مالی در سطح بین‌المللی را با مشکلات جدی مواجه می‌کند و وضعیت امنیت اقتصادی و ملی آن کشور را تنزل می‌دهد.

## راهکارهای پیشنهادی

در واقع، در فرآیند پول‌شویی تلاش بر آن است تا درآمدها و عواید حاصل از فعالیت‌های غیرقانونی شسته و به درآمدهای قانونی و مشروع تبدیل شود. ازاین‌رو، گام نخست در جهت اتخاذ سیاست‌های ضد پول‌شویی، سیاست‌گذاری صحیح و استفاده از ابزارها و روش‌های کارآ برای از بین بردن زمینه‌ها و مبارزه با جرایم اولیه منتهی به پول‌شویی است. به‌علاوه، همان‌طور که بیان شد، به دنبال پیشرفت‌های سریع در حوزه رایانه و فناوری اطلاعات، روش‌های پول‌شویی سایبری از پیچیدگی‌های بالایی برخوردار است و بنابراین، با استفاده از ابزارهای عادی تشخیص پول غیرقانونی نمی‌توان با این نوع پول‌شویی مقابله کرد. بنابراین، کارشناسان معتقدند، سیاست‌ها و اقدام‌های ضد پول‌شویی باید به‌گونه‌ای طراحی شوند که ابعاد مختلف فناوری اطلاعات، سازمانی، فنی و حقوقی را دربر گیرند. از جمله راهکارهای پیشنهادی در این چهارچوب می‌توان به پنج مقوله اصلی زیر اشاره کرد:

**۱- شناسایی معاملات مالی مشکوک به پول‌شویی سایبری:** در این چهارچوب می‌توان گفت، مشتریان دارای روابط کاری با بانک‌ها یا استفاده‌کنندگان از خدمات از راه دور با استفاده از فناوری‌های مدرن از جمله گروه‌هایی هستند که در معرض ریسک بالای پول‌شویی قرار دارند. بنابراین، شناسایی معاملات مالی مشکوک در فضای بانک‌داری الکترونیک و فضای مجازی بسیار مهم است. انجام هریک از اقدام‌های زیر می‌تواند از جمله نشانه‌های تلاش برای ارتکاب جرم پول‌شویی توسط مشتریان باشد که لازم است به‌دقت مورد پی‌گیری قرار گیرد:

- تلاش برای ورود از طریق IP نشانی جدید یا بسته شده (ممنوع).

- تلاش برای استفاده از کلیدهای قدیمی، کلیدهای عملیاتی یا کلیدهای اولیه منقضی‌شده بعد از تأیید یک کلید جدید.
- استفاده از معاملات بانکی IP نشانی‌ها یا نام‌های استفاده‌کننده‌ای که براساس نظارت‌های اولیه مربوط به درگیر بودن در معاملات کلاهبرداری، مشکوک بوده‌اند.
- اجرای معاملات در زمان نامعمول یا وصل شدن به سیستم در خارج از زمان کاری.
- شرایط غیرعادی یا پیچیدگی‌های نامعمول در معاملات؛ برای مثال، انجام تعداد زیادی از انتقالات از یک حساب در دوره کوتاهی از زمان یا استفاده از منابع یا روش‌های پرداخت (ابزارهای) مختلف برای انجام انتقالات مالی.
- استفاده از افرادی که از ماهیت فعالیت نهادهای به‌ظاهر قانونی که آنها را نمایندگی می‌کند، مطلع نیستند.
- افرادی که نمی‌توانند دلیل نیازشان به خدمات بانک‌داری خاص را توضیح دهند.
- درگیر شدن در اجرای معاملات افراد جوان یا کسب‌وکارهای تازه‌تأسیس.
- اجرای معاملات با استفاده از اسناد مفقودی.
- باز کردن حسابی که به دلیل بدهی غیرمجاز خیلی زود اعتبار آن افزایش می‌یابد.
- تلاش برای برداشت وجوه در روز دریافت اعتبار.
- تلاش مشتری برای دست یافتن به دو کارت اعتباری یا بیشتر وقتی این عمل با ماهیت کسب‌وکار یا گردش کاری او ناسازگار است.
- اعتباردهی وجوه به حساب‌های دارای کارتی که بلافاصله این اعتبار از دستگاه خودپرداز (شامل طرف‌های سوم) از آن حساب برداشت می‌شود.
- اجرای معاملاتی که نسبت به معاملات قبلی مشتری متفاوت هستند.
- کمبود اطلاعات در مورد فعالیت‌های کسب‌وکار مشتری یا استفاده از سیستم‌های پرداخت آنلاین به‌جای سیستم‌های پرداخت متعارف.
- انتقالات بین‌المللی عادی که با فعالیت کسب‌وکار مشتری سازگار هستند.
- رابطه نامعلوم بین فرستنده خارجی پول و دریافت‌کننده انفرادی آن.
- حواله‌های خصوصی برای افراد خصوصی که دارای فعالیت‌های تجاری احتمالی هستند (یعنی بیت‌کوین‌ها یا ارایه‌دهندگان خدمات تبادل پول تحت وب و...).
- نقل‌وانتقال وجوه از طریق مشتری به حساب بانکی شخص دیگر با استفاده از دسترسی از راه دور.
- معاملات بین مرزی که با استفاده از حواله‌ها یا بانک‌داری اینترنتی اجرا می‌شوند.
- نقل‌وانتقال وجوه به/ از مکان‌های دور که ارتباط آشکار یا مستقیم با فعالیت‌ها یا حساب مشتری ندارند.
- درگیری تعداد زیادی از طرف‌های سوم خارجی (افراد و نهادهای قانونی) در انجام معاملات.
- استفاده از شرکت‌های جعلی.

- توجه به اطلاعات ارایه شده از FIUs[1] و پلیس.

**۲- حمایت قانونی برای جلوگیری (از) و مقابله با قانونی کردن عواید جرایم سایبری:** از جمله مواردی که در تصویب قوانین ضد پول‌شویی باید مورد توجه قرار گیرند، عبارت‌اند از:

- الزام پاسخگویی واحد فناوری اطلاعات و رایانه که جرایم از طریق آنها صورت گرفته است.
- الزام به معرفی و شناسایی از طریق تماس رودررو با مشتریانی که از خدمات دسترسی از راه دور یا سیستم پرداخت الکترونیک استفاده می‌کنند.
- مجاز بودن استفاده از اسناد و سایر داده‌های الکترونیکی به‌عنوان مدرک در بررسی جرایم سایبری.
- کاهش تعداد پرداخت‌ها و انتقال وجوه ناشناس.
- الزام به دریافت مجوز برای ابزارهای پرداخت الکترونیکی.
- ایجاد سازوکارهای روشن در مورد تعامل بین مشتری و بانک و همچنین بین بانک ذی‌نفع و بانک فرستنده در مورد بدهی غیرمجاز حساب مشتری.

**۳- اقدام‌های ضد پول‌شویی فنی و سازماندهی شده توسط بانک‌ها:** از جمله این اقدام‌ها عبارت‌اند از:

- بازرسی منظم خودپردازها به‌منظور بررسی وجود هرگونه دستگاهی (سخت‌افزاری) که به‌طور غیرقانونی روی آنها نصب شده است.
- ارایه کارت‌های پلاستیکی مشتری با فناوری ریزتراشه تعبیه شده روی آنها برای حمایت بهتر در برابر جعل.
- تهیه فهرست سیاه از حساب‌های کلاهبرداران (کدهای شناسایی، IP نشانی‌ها و...) برای اطمینان از تعلیق سریع معاملات.
- ارایه احراز هویت دوکاناله یا دوعامله.
- استفاده از توکن‌ها برای ذخیره امضاهای دیجیتال.
- الزام مشتریان به اطلاع‌رسانی در مورد همه معاملات اجرا شده در حساب آنها.
- تأیید پرداخت از طریق تلفن.
- مشارکت مشتری در ایجاد کلید مشتری به‌عنوان وسیله‌ای برای جلوگیری از هرنوع تخلف از سوی کارمندان بانک.
- پیوند کلید مشتری با شماره سریال دیسک فلاپی، درایو فلش یا دیسک سخت این امکان را فراهم می‌کند که کلیدهای بانک- مشتری را کپی کند یا به صفحه مشتری از سایر رایانه‌ها قابل دسترسی باشد.
- استفاده از قواعد منطقی چندگانه برای پرداخت‌های سیستمی بانک - مشتری معمولی، تعلیقی یا غیرمعمولی.
- استفاده از سیستم بانک - مشتری (بانک‌داری اینترنتی) با فیلترهای خطی سفارشی‌شده.
- استفاده از تحلیل‌های آماری ترافیک (جریان خالص) در مورد حضور ناهنجاری‌ها.
- وضع محدودیت برای معاملات آنلاین.

1- Financial Intelligence Units

- وضع محدودیت‌ها بر معاملات اجرا شده در حوزه‌های قضایی دارای ریسک بالا.
- وضع محدودیت بر فراوانی معاملات.

**۴- افزایش آگاهی عمومی در مورد جرایم پول‌شویی سایبری:** باید توجه کرد، سیاست‌گذاری در مورد فعالیت‌هایی که افزایش آگاهی عمومی را در مورد ریسک‌ها و تهدیدهایی که سیستم‌های رایانه‌ای و پرداخت شبکه‌ای به همراه دارند، می‌تواند نقش مهمی در پیشگیری از وقوع جرایم پول‌شویی به همراه داشته باشد. از جمله مهم‌ترین عواملی که موجب ناآگاهی عمومی در مورد جرایم پول‌شویی سایبری شده است می‌توان به موارد زیر اشاره کرد:

- دسترسی محدود به اطلاعات در مورد جرایم سایبری.
- آگاهی اندک در مورد ریسک‌هایی که توسط سیستم‌ها و خدمات پرداخت جدید ایجاد می‌شوند.
- آگاهی اندک در مورد ریسک‌های مربوط به پول‌شویی.
- نصب و استفاده از نرم‌افزارهای بدون مجوز (سیستم‌های عملیاتی، آنتی ویروس‌ها و...).
- ذخیره ناامن امضاهای دیجیتال و کدهای دسترسی (پسوردها) توسط مشتریان بانک.
- نقض قواعد اساسی ایمنی برای استفاده از بانک‌داری اینترنتی و ابزارهای پرداخت آنلاین.
- عدم رعایت کد (پسورد) و سیاست امنیت اطلاعات.

بنابراین، الزام نهادها و بانک‌ها به مدیریت ایمن داده‌های الکترونیکی، اتخاذ اقدام‌هایی برای مقابله با دسترسی به این اطلاعات و استفاده از نرم‌افزارهای ضد هک و ضد ویروس مجوزدار در سیستم‌های پرداخت سایبری می‌تواند بسیار مفید باشد.

**۵- بهبود چهارچوب قانونی و نظارتی بر امنیت اطلاعات:** بهبود چهارچوب قانونی و نظارتی بر امنیت اطلاعات چه در سطح خصوصی و چه در سطح دولتی مهم است. در این ارتباط، نهادها و شرکت‌های خصوصی و دولتی می‌توانند پیش‌نویس نظارت‌های داخلی را تهیه کنند که برمبنای آن کارمندان به‌طور قانونی از همکاری با مجرمان پول‌شویی منع شوند. همچنین دسترسی به اطلاعاتی که دربردارنده موضوع‌های سری دولتی، بانک‌داری و... است باید تنها ۱- به کارمندانی داده شود که لازمه اجرای وظایف کاری آنها استفاده از چنین اطلاعاتی است. ۲- افرادی که از نظر قانونی یا برحسب وظیفه مجاز به دسترسی به این اطلاعات باشند. این پیش‌نویس همچنین می‌تواند دربردارنده الزام به اعمال نظارت و کنترل مناسب بر رعایت دستورالعمل‌های امنیت اطلاعات باشد.

**سیستم‌های پرداخت الکترونیک با استفاده از پول الکترونیک عمل می‌کنند، یعنی یک ابزار مالی که به کاربر اجازه می‌دهد تا حق مطالبه را با استفاده از حساب‌های مجازی و سوابق الکترونیکی (ایمیل و...) مبادله یا به پول نقد و ابزارهای با نقدینگی بالای دیگر تبدیل کند.**

## منابع

- انصاری پیرسرایی، زربخش و اسداله شاه بهرامی (۱۳۹۳)، «ضرورت استفاده از سیستم‌های تشخیص پول‌شویی در بانک‌داری الکترونیکی»، فصلنامه روند، سال بیست‌ویکم، شماره ٦٨، صص ۱۷۹-۲۱۲.
- سایت خبری ایلنا، کد خبر: ٨٦٢٥٦٩.
- شمس‌آبادی، پریسا (۱۳۸۷)، «پول‌شویی و اثرات آن بر روی سیستم مالی»، اداره تحقیقات، کنترل ریسک و تطبیق بانک سپه.
- کشتکار، مریم (۱۳۹۰)، «راهکارهای مبارزه با پول‌شویی در بانک‌ها و مؤسسات اعتباری، فصلنامه تازه‌های اقتصادی»، سال نهم، شماره ۱۳۲.
- مسلمی پطرودی، محسن (۱۳۹۵)، «پارادایم پول‌شویی در ایران»، پنجمین کنفرانس بین‌المللی پژوهش‌های نوین در مدیریت، اقتصاد و حسابداری.
- معدنی، جواد و داود حسین‌پور (۱۳۹۸)، «تدوین الگوی مبارزه با پول‌شویی با استفاده از رویکرد خط‌مشی‌گذاری تعاملی»، فصلنامه علمی مطالعات راهبردی سیاست‌گذاری عمومی، دوره ۹، شماره ۳۰، صص ٦٨- ٤٣.
- نصرالهی، زهرا و ندا حکیمی (۱۳۹۵) «بررسی روند حجم پول‌شویی و تأثیر آن بر مصرف در ایران: رویکرد مدل ساختاری با کاربرد نرم‌افزار آموس گرافیک»، فصلنامه اقتصاد مقداری، دوره ۱۳، شماره ٤، صص ۱۵۷- ۱۳۵.

-Cybercrime and money laundering (2014), Eurasian group on combating money laundering and financing of terrorism.

– Rahmdel, Mansour (2018), FATF and Money Laundering in Iran, journal of money laundering control.

-The Most Popular Money Laundering Methods in Cybercrime, https://calert.info.

– Basel AML index, International Centre for asset recovery.

سیستم‌های پرداخت الکترونیک با استفاده از پول الکترونیک عمل می‌کنند، یعنی یک ابزار مالی که به کاربر اجازه می‌دهد تا حق مطالبه را با استفاده از حساب‌های مجازی و سوابق الکترونیکی (ایمیل و...) مبادله یا به پول نقد و ابزارهای با نقدینگی بالای دیگر تبدیل کند.