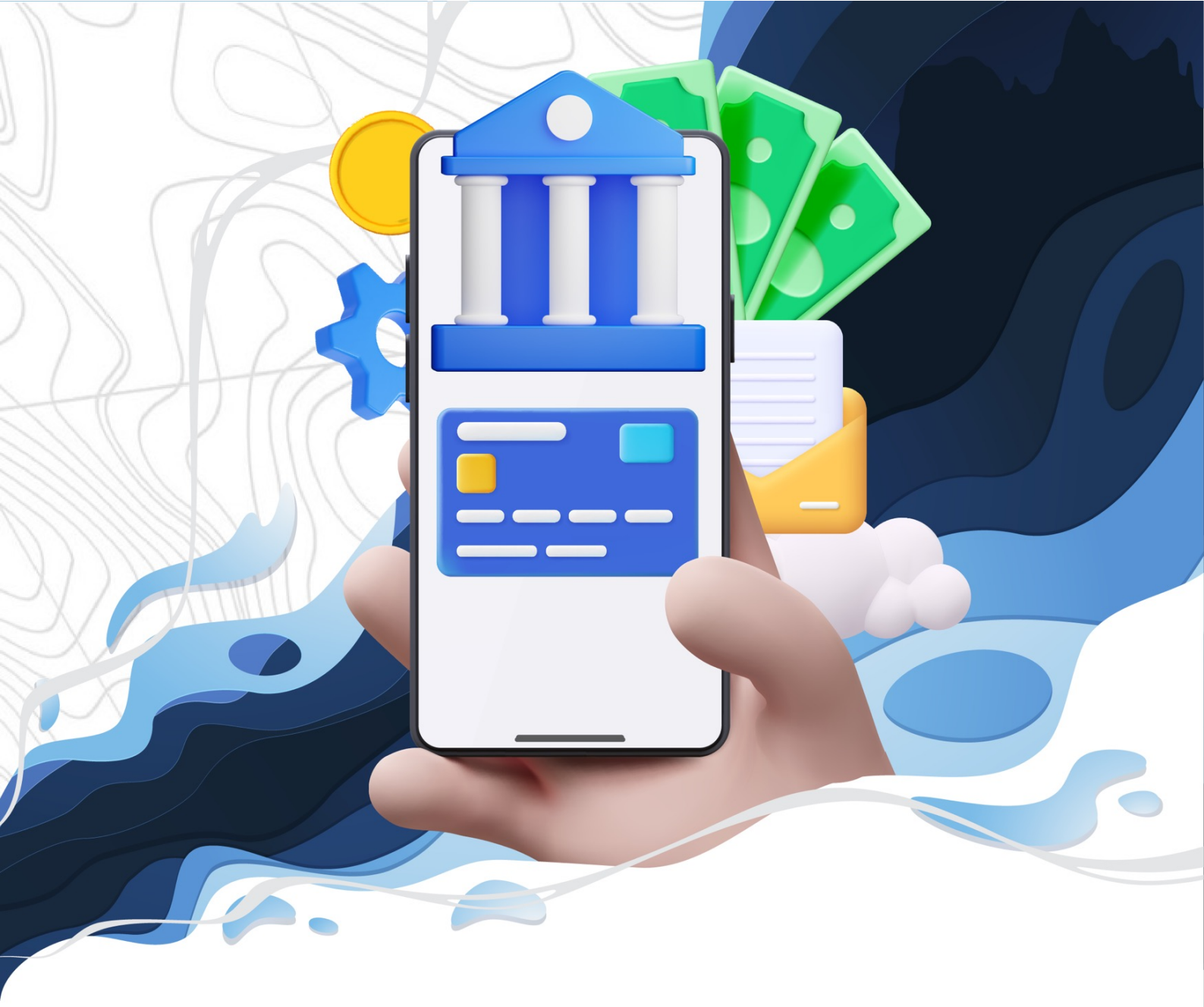


PENGKINIAN KAJIAN TIPOLOGI 2023

TINDAK PIDANA PENCUCIAN UANG, TINDAK PIDANA PENDANAAN TERORISME DAN PENDANAAN PROLIFERASI SENJATA PEMUSNAH MASSAL

BANK INDONESIA

2023

PENGANTAR DEPUTI GUBERNUR BANK INDONESIA

Puji syukur kita panjatkan kepada Tuhan Yang Maha Kuasa karena hanya berkat rahmat dan kehendak-Nya, Kajian Tipologi Tindak Pidana Pencucian Uang, Tindak Pidana Pendanaan Terorisme, dan Pendanaan Proliferasi Senjata Pemusnah Massal pada Sektor Penyedia Jasa Pembayaran Lembaga Selain Bank dan Kegiatan Usaha Penukaran Valuta Asing Bukan Bank dapat tersusun dengan baik.

Bank Indonesia berkomitmen sepenuhnya untuk mendukung upaya pencegahan dan pemberantasan tindak pidana pencucian uang, pendanaan terorisme, dan pendanaan senjata pemusnah massal melalui peran Bank Indonesia sebagai Lembaga Pengawas dan Pengatur yang tergabung dalam Komite Koordinasi Nasional Pencegahan dan Pemberantasan TPPU.

Dalam rangka melaksanakan perannya, Bank Indonesia menetapkan aturan, memberikan serta mencabut izin, melakukan pengawasan, dan memberikan sanksi terhadap Penyedia Jasa Pembayaran Lembaga Selain Bank dan Kegiatan Usaha Penukaran Valuta Asing Bukan Bank yang berada di bawah wewenangnya, sesuai dengan peraturan perundang-undangan.

Saat ini, sektor sistem pembayaran menghadapi risiko yang semakin kompleks dan beragam terkait pencucian uang, pendanaan terorisme, dan pendanaan proliferasi senjata pemusnah massal. Oleh karena itu, dibutuhkan sebuah panduan yang dapat memberikan gambaran tentang berbagai modus dan tipologi yang dilakukan oleh para pelaku kejahatan untuk mengurangi risiko dari aktivitas tersebut.

Saya mengapresiasi penyusunan kajian tipologi ini untuk meningkatkan *awareness* Penyedia Jasa Pembayaran Lembaga Selain Bank dan Kegiatan Usaha Penukaran Valuta Asing Bukan Bank sebagai salah satu referensi yang mampu mengoptimalkan upaya mitigasi yang dilakukan agar tidak menjadi sarana dan sasaran bagi pelaku

pencucian uang, pendanaan terorisme, dan pendanaan proliferasi senjata pemusnah massal. Lebih lanjut, Bank Indonesia berkomitmen untuk terus memperbarui dan menyempurnakan kajian ini sesuai dengan perkembangan risiko pencucian uang, pendanaan terorisme, dan pendanaan proliferasi senjata pemusnah massal terkini yang dihadapi oleh industri sistem pembayaran.

Adapun dalam suatu upaya pencegahan yang dilakukan ini diharapkan dapat berkontribusi dalam pengembangan integrasi sistem keuangan, peningkatan kepercayaan dan reputasi Indonesia, serta bentuk kepatuhan terhadap standar internasional termasuk rekomendasi Financial Action Task Force (FATF).

Semoga Tuhan Yang Maha Kuasa merestui dan meringankan langkah kita dalam memberikan kontribusi nyata yang terbaik untuk bangsa, negara, dan masyarakat. Sekian dan terima kasih.

Deputi Gubernur Bank Indonesia

Filianingsih Hendarta

RINGKASAN EKSEKUTIF

Berdasarkan Rekomendasi Financial Action Task Force (FATF) Nomor 1, disebutkan bahwa setiap negara diharuskan untuk melakukan identifikasi, analisis, dan evaluasi terhadap risiko Tindak Pidana Pencucian Uang (TPPU), Tindak Pidana Pendanaan Terorisme (TPPT), dan Pendanaan Proliferasi Senjata Pemusnah Massal (PPSPM) di negara tersebut. Sehubungan dengan perkembangan zaman, praktik pencucian uang, pendanaan terorisme, dan pendanaan proliferasi senjata pemusnah massal juga semakin kompleks dan berkembang. Dengan demikian, diperlukan penelitian untuk melihat tipologi yang dilakukan oleh para pelaku dalam melancarkan aksi pencucian uang, pendanaan terorisme, dan pendanaan proliferasi senjata pemusnah massal.

Kajian Tipologi ini diharapkan dapat menjadi panduan bagi otoritas terkait maupun Penyedia Jasa Pembayaran (PJP) Lembaga Selain Bank dan Kegiatan Usaha Penukaran Valuta Asing (KUPVA) Bukan Bank yang berada di bawah pengaturan dan pengawasan Bank Indonesia, untuk mengidentifikasi tipologi yang dilakukan oleh pelaku pencucian uang, pendanaan terorisme, dan pendanaan proliferasi senjata pemusnah massal. Pemahaman terhadap tipologi perlu dikembangkan juga dengan mendalami tipologi berdasar tindak pidana asal terutama penipuan siber, perpajakan, bea cukai, narkotika, korupsi, kehutanan, dan lingkungan hidup.

Berdasarkan analisis tipologi tersebut, penyelenggara diharapkan dapat meningkatkan mitigasi yang tepat atas risiko TPPU, TPPT, dan PPSPM melalui penguatan implementasi Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme APU PPT berbasis risiko *(risk based approach).*

Berdasarkan hasil Kajian Tipologi TPPU, TPPT, PPSPM diperoleh beberapa informasi, sebagai berikut:

1. Berdasarkan data salinan putusan pengadilan tahun 2015-2020, terdapat 29 (dua puluh sembilan) kasus yang berkaitan dengan TPPU dan TPPT.

Dari total putusan tersebut, sebanyak 24 (dua puluh empat) putusan merupakan perkara TPPU, sedangkan 5 (lima) putusan merupakan perkara TPPT. Pada data putusan pengadilan tahun 2015-2020 tidak ditemukan kasus yang berkaitan dengan PPSPM. Adapun dari putusan tersebut diperoleh beberapa informasi sebagai berikut:

a. Profil pekerjaan pelaku yang dominan dari kasus TPPU dan TPPT selama tahun 2015- 2020 yaitu:

    1. Pada perkara TPPU, profil pekerjaan pelaku yang dominan adalah Wiraswasta yaitu sebanyak 16 (enam belas) orang pelaku. Sementara itu, profil pekerjaan lainnya adalah Pegawai Swasta, PNS, Pejabat Pemerintahan, Ibu Rumah Tangga, Pegawai *Money Changer*, Pengajar, dan lainnya.
    2. Pada perkara TPPT, terdapat pelaku yang profil pekerjaannya adalah Wiraswasta. Selain itu, terdapat pelaku yang tidak bekerja, serta pelaku yang tidak dapat diidentifikasi profil pekerjaannya.

b. Profil badan usaha yang dominan dari kasus TPPU dan TPPT selama tahun 2015-2020 yaitu:

    1. Pada perkara TPPU, profil badan usaha yang terlibat didominasi oleh Perusahaan Non UMKM berbentuk PT, yaitu sebanyak 11 (sebelas) kasus. Profil badan usaha lainnya adalah CV. Selain itu, terdapat kasus yang tidak dapat diidentifikasi profil badan usahanya.
    2. Pada perkara TPPT, tidak dapat diidentifikasi profil badan usaha yang terlibat.

c. Berdasarkan karakteristik sebaran wilayah dari kasus TPPU dan TPPT selama tahun 2015-2020 yaitu:

   1. Pada perkara TPPU, sebagian besar perkara berada di DKI Jakarta, yaitu sebanyak 20 (dua puluh) kasus. Adapun sebaran wilayah lainnya yaitu Kalimantan Barat, Banten, dan Lampung.

   2. Pada perkara TPPT, sebagian besar perkara berada di DKI Jakarta, yaitu sebanyak 3 (tiga) kasus. Meskipun demikian, terdapat juga kasus yang tidak dapat diidentifikasi wilayahnya.

d. Produk dan layanan yang digunakan dalam kasus TPPU dan TPPT selama tahun 2015- 2020 yaitu:

   1. Pada perkara TPPU, produk dan layanan yang dominan digunakan pada KUPVA Bukan Bank adalah produk Uang Kertas Asing (UKA) USD, diikuti SGD, dan EUR. Sementara itu, mekanisme jual beli UKA yang dominan digunakan adalah Transfer Bank. Sedangkan pada Penyelenggara Transfer Dana (PTD) Selain Bank, produk dan layanan yang dominan digunakan yaitu *Account to Account (Incoming)*, dan *Cash to Account (Outgoing)*.

   2. Pada perkara TPPT, produk dan layanan yang dominan digunakan pada KUPVA Bukan Bank adalah produk UKA USD. Sedangkan pada PTD Selain Bank, produk dan layanan yang dominan digunakan yaitu *Cash to Account (Outgoing),* diikuti *Account to Account (Outgoing).*

e. *Delivery channel* yang digunakan dalam kasus TPPU dan TPPT selama tahun 2015- 2020 yaitu:

   1. Pada perkara TPPU, *delivery channel* yang dominan digunakan adalah Kantor KUPVA Bukan Bank, yaitu sebanyak 22 (dua puluh dua) kasus. Untuk *delivery channel* lainnya yang digunakan adalah Kantor PTD Bukan Bank.

   2. Pada perkara TPPT, *delivery channel* yang dominan digunakan adalah Kantor PTD Bukan Bank, yaitu sebanyak 4 (empat) kasus. Untuk *delivery channel* lainnya yang digunakan adalah Kantor KUPVA Bukan Bank.

2. Berdasarkan data hasil survei yang dilakukan pada penyelenggara KUPVA Bukan Bank, PTD Selain Bank, Penyelenggara Uang Elektronik (UE) dan Dompet Elektronik (DE) Selain Bank, serta Penyelenggara Alat Pembayaran Menggunakan Kartu (APMK) Selain Bank, didapatkan bahwa:

   a. Tipologi TPPU dan TPPT pada penyelenggara KUPVA Bukan Bank, antara lain:

      1. Terdapat 3 (tiga) tipologi TPPU yang memiliki risiko tertinggi pada KUPVA Bukan Bank yaitu penggunaan identitas palsu, *mingling*, serta *trade-based money laundering* dan *transfer pricing*.

      2. Terdapat 3 (tiga) tipologi TPPT yang memiliki risiko tertinggi pada KUPVA Bukan Bank yaitu Penggunaan Dana: Operasi Terorisme Domestik— Pembelian Senjata dan Bahan Peledak, Penggunaan Dana: Operasi Terorisme Domestik— Dokumen Identitas Palsu, Penggunaan Dana: Operasi Terorisme Domestik— Perjalanan dari dan ke lokasi aksi terorisme.

b. Tipologi TPPU dan TPPT pada PTD Selain Bank, antara lain:

   1. Terdapat 3 (tiga) tipologi TPPU yang memiliki risiko tertinggi pada PTD Selain Bank yaitu *smurfing*, aktivitas perjudian *online*, dan *structuring*.

   2. Terdapat 3 (tiga) tipologi TPPT yang memiliki risiko tertinggi pada PTD Selain Bank yaitu Pengumpulan Dana—Ilegal: Hasil Kejahatan Kriminal Lainnya, Penggunaan Dana: Operasi Terorisme Domestik—Dokumen Identitas Palsu, Penggunaan Dana: Operasi Terorisme Domestik—Perjalanan dari dan ke lokasi aksi terorisme.

c. Tipologi TPPU dan TPPT pada penyelenggara UE dan DE Selain Bank, antara lain:

   1. Terdapat 3 (tiga) tipologi TPPU yang memiliki risiko tertinggi pada penyelenggara UE dan DE Selain Bank yaitu penggunaan identitas palsu, *smurfing*, dan aktivitas perjudian *online*.

   2. Terdapat 3 (tiga) tipologi TPPT yang memiliki risiko tertinggi pada penyelenggara UE dan DE Selain Bank yaitu Pengumpulan Dana—Ilegal: Penculikan dengan Tebusan, Pengumpulan Dana—Ilegal: Hasil Kejahatan Kriminal Lainnya, dan Penggunaan Dana: Operasi Terorisme Domestik—Perjalanan dari dan ke lokasi aksi terorisme.

d. Tipologi TPPU dan TPPT pada penyelenggara APMK Selain Bank, antara lain:

   1. Terdapat 3 (tiga) tipologi TPPU yang memiliki risiko tertinggi pada penyelenggara APMK Selain Bank yaitu penggunaan identitas palsu, pemanfaatan internet enkripsi, akses terhadap identitas, perbankan internasional, serta pemanfaatan Kartu Kredit, Cek, Surat Perjanjian Hutang.

   2. Terdapat 3 (tiga) tipologi TPPT yang memiliki risiko tertinggi pada penyelenggara APMK Selain Bank yaitu Pengumpulan Dana—Legal: Sponsor Pribadi *(Terrorist Financier/ Fundraiser)*, Pengumpulan Dana—Legal: Penyimpangan Pengumpulan Donasi Melalui Ormas, Pengumpulan Dana—Legal: Pendanaan *Crowdfunding*.

3. Berdasarkan data hasil survei yang dilakukan pada penyelenggara KUPVA Bukan Bank, PTD Selain Bank, Penyelenggara UE dan DE Selain Bank, serta Penyelenggara APMK Selain Bank, tidak ditemukan adanya modus/tipologi yang berkaitan dengan PPSPM. Meskipun demikian, berdasarkan hasil penelitian dari berbagai sumber literatur ditemukan beberapa tipologi yang berkaitan dengan PPSPM yaitu:

   1. Transaksi ekspor-impor yang melibatkan barang-barang yang dikendalikan dalam rezim kontrol ekspor PPSPM;

   2. Transaksi melibatkan entitas yang memiliki hubungan dengan negara yang rentan terhadap praktik PPSPM;

   3. Penggunaan *front company* dalam transaksi;

   4. Transaksi yang dilakukan antar perusahaan;

   5. Transaksi menggunakan *wire transfer*;

   6. Transaksi melibatkan orang atau entitas dari luar negeri yang ditujukan untuk menyamarkan aliran dana;

   7. Penggunaan dokumen, alamat, dan nomor telepon yang sama dengan milik suatu perusahaan untuk melakukan pembukaan rekening dan mendirikan *Front Company*;

   8. Transaksi menggunakan logam mulia;

9. Keterlibatan perusahaan perdagangan kecil atau perusahaan perantara yang melakukan kegiatan bisnis tidak sesuai dengan kegiatan usahanya;
10. Perusahaan yang melakukan pengiriman uang;
11. Transaksi menggunakan dokumen fiktif atau tidak valid;
12. Transaksi melibatkan negara yang rentan terhadap aktivitas proliferasi;
13. Pembayaran transaksi dilakukan oleh entitas lain;
14. Perusahaan dijalankan oleh keluarga yang memiliki alamat bisnis dan akun *email* yang sama;
15. Perusahaan menggunakan rekening yang sama untuk bertransaksi;
16. Transaksi tanpa disertai dengan dokumen pendukung, seperti faktur atau rincian lainnya;
17. Transaksi yang melibatkan individu atau entitas dari negara yang rentan dengan praktik PPSPM;
18. Transaksi menggunakan identitas palsu;
19. Pengguna jasa memberikan informasi yang tidak valid, terutama yang berkaitan dengan barang atau jasa yang di ekspor;
20. Transaksi menggunakan informasi fiktif terkait lokasi pengiriman;
21. Transaksi melibatkan perusahaan ekspor.

Daftar **Isi**

Daftar Tabel

Daftar Grafik

Daftar Gambar

Daftar Singkatan

No	Singkatan	Penjelasan
1	APMK	Alat Pembayaran Menggunakan Kartu
2	APU PPT	Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme
3	CDD	*Customer Due Diligence*
4	CV	Persekutuan Komanditer
5	DE	Dompet Elektronik
6	Dukcapil	Kependudukan dan Catatan Sipil
7	e-CDD	*Electronic Customer Due Diligence*
8	*E-Commerce*	*Electronic Commerce*
9	EDC	*Electronic Data Capture*
10	EUR	Euro
11	FATF	Financial Action Task Force on Money Laundering
12	FTF	*Foreign Terrorist Fighter*
13	ISIS	*Islamic State of Iraq and Suriah*
14	KHR	Cambodian Riel
15	Komite TPPU	Komite Koordinasi Nasional Pencegahan dan Pemberantasan TPPU
16	KUPVA	Kegiatan Usaha Penukaran Valuta Asing
17	KYC	*Know Your Customer*
18	LPP	Lembaga Pengawas dan Pengatur
19	MYR	Malaysian Ringgit
20	NPO	*Non Profit Organization*
21	Ormas	Organisasi Kemasyarakatan
22	PBB	Perserikatan Bangsa-Bangsa
23	PEP	*Politically Exposed Persons*
24	PHP	Philippine Peso
25	PJP	Penyedia Jasa Pembayaran
26	PNS	Pegawai Negeri Sipil
27	PPP	*Public Private Partnership*
28	PPSPM	Pendanaan Proliferasi Senjata Pemusnah Massal
29	PT	Perseroan Terbatas

No	Singkatan	Penjelasan
30	PTD	Penyelenggara Transfer Dana
31	*Regtech*	*Regulatory Technology*
32	SGD	Dolar Singapura
33	*Suptech*	*Supervisory Technology*
34	T/T	*Telegraphic Transfer*
35	TKI	Tenaga Kerja Indonesia
36	TPPT	Tindak Pidana Pendanaan Terorisme
37	TPPU	Tindak Pidana Pencucian Uang
38	UE	Uang Elektronik
39	UKA	Uang Kertas Asing
40	UMKM	Usaha Mikro Kecil Menengah
41	USD	Dolar Amerika Serikat
42	UU	Undang-Undang
43	VND	Vietnamese Dong
44	WMD	*Weapon Mass Destruction*
45	WNA	Warga Negara Asing
46	PJK	Penyedia Jasa Keuangan

BAGIAN 1

PENDAHULUAN

1.1 Latar Belakang

Indonesia sebagai bagian dari masyarakat dunia bersikap terbuka dalam menjalin hubungan dengan negara lain, termasuk keterbukaan lalu lintas keuangan antar negara yang memberikan kemudahan dalam bertransaksi. Hal ini tentunya memiliki dampak positif dari sisi perekonomian, namun demikian tidak dapat dipungkuri bahwa hal tersebut juga menimbulkan risiko terhadap sistem keuangan Indonesia. Adapun risiko yang dimaksud berkaitan dengan praktik Tindak Pidana Pencucian Uang (TPPU), Tindak Pidana Pendanaan Terorisme (TPPT), dan Pendanaan Proliferasi Senjata Pemusnah Massal (PPSPM). Keterbukaan akses untuk bertransaksi dapat dengan mudah disalahgunakan oleh orang-orang yang tidak bertanggung jawab dalam mendukung aksi kejahatannya. Lebih lanjut, permasalahan kurangnya koordinasi dan sosialisasi antar lembaga, lemahnya pengawasan dan penegakan hukum, serta sulitnya proses identifikasi terhadap identitas dan asal usul dana hasil kejahatan, menjadi faktor yang mempermudah pelaku dalam melancarkan aksinya.

Tindak pidana pencucian uang, pendanaan terorisme, dan pendanaan proliferasi senjata pemusnah massal pada akhirnya dapat mengancam stabilitas perekonomian, integritas sistem keuangan, serta membahayakan sendi-sendi kehidupan bermasyarakat, berbangsa, dan bernegara. Sehubungan dengan itu, Bank Indonesia berkomitmen penuh untuk mendukung langkah-langkah Pemerintah Republik Indonesia dalam pencegahan TPPU, TPPT, serta PPSPM melalui peran Bank Indonesia sebagai Lembaga Pengawas dan Pengatur (LPP) sesuai ketentuan perundang-undangan terkait TPPU dan TPPT, serta selaku anggota Komite Koordinasi Nasional Pencegahan dan Pemberantasan TPPU (Komite TPPU). Dalam konteks ini, Bank Indonesia menetapkan peraturan, memberikan dan mencabut izin, melaksanakan pengawasan, serta mengenakan sanksi terhadap Penyedia Jasa Pembayaran (PJP) Lembaga Selain Bank dan Kegiatan Usaha Penukaran Valuta Asing (KUPVA) Bukan Bank yang berada di bawah kewenangan Bank Indonesia. Komitmen Bank Indonesia dalam pencegahan TPPU, TPPT, dan PPSPM juga diwujudnyatakan dalam Visi ke-4 *Blueprint* Sistem Pembayaran 2025 yaitu menjamin keseimbangan antara inovasi dengan perlindungan konsumen, integritas dan stabilitas serta persaingan usaha yang sehat melalui penerapan prinsip *Know Your Customer* (KYC) serta Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU PPT), kewajiban keterbukaan data/informasi/bisnis publik, serta penerapan *Regulatory Technology (Regtech)* dan *Supervisory Technology* (*Suptech)* dalam kewajiban pelaporan, regulasi dan pengawasan.

Dalam rezim upaya pencegahan dan pemberantasan TPPU, TPPT, dan PPSPM di Indonesia, Bank Indonesia selaku LPP serta penyelenggara di bawah pengaturan dan pengawasan Bank Indonesia memiliki kewajiban untuk menjaga industri sistem pembayaran termasuk KUPVA Bukan Bank agar tidak menjadi sarana dan sasaran bagi pelaku pencucian uang, pendanaan terorisme, dan pendanaan proliferasi senjata pemusnah massal. Namun demikian, dalam perkembangannya, modus TPPU, TPPT, dan PPSPM semakin kompleks dan semakin variatif sesuai dengan tindak pidana asalnya. Oleh karena itu, sebagai salah satu langkah mitigasi, diperlukan suatu panduan yang diharapkan dapat memberikan gambaran mengenai modus/tipologi yang dilakukan oleh para pelaku TPPU, TPPT, dan PPSPM di sektor sistem pembayaran. Dalam hal ini Bank Indonesia melakukan penyusunan analisis tipologi TPPU, TPPT, dan PPSPM dengan basis data berupa putusan pengadilan atas perkara TPPU, TPPT, dan PPSPM yang melibatkan penyelenggara di bawah kewenangan Bank Indonesia. Penelitian ini diharapkan dapat menjadi landasan dalam mitigasi potensi risiko TPPU, TPPT, dan PPSPM oleh penyelenggara yang berada di bawah pengaturan dan pengawasan Bank Indonesia.

1.2 Perumusan Masalah

Rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana karakteristik dari kasus-kasus TPPU, TPPT, dan PPSPM berdasarkan putusan pengadilan atas perkara TPPU, TPPT, dan PPSPM yang melibatkan PJP Lembaga Selain Bank dan KUPVA Bukan Bank selama periode tahun 2015-2020?
2. Bagaimana tipologi dari kasus-kasus TPPU, TPPT, dan PPSPM yang melibatkan PJP Lembaga Selain Bank dan KUPVA Bukan Bank berdasarkan putusan pengadilan selama periode tahun 2015-2020?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui karakteristik profil pengguna jasa (perorangan dan badan usaha), wilayah, produk dan layanan, serta *delivery channel* berdasarkan putusan pengadilan atas perkara TPPU, TPPT, dan PPSPM yang melibatkan PJP Lembaga Selain Bank dan KUPVA Bukan Bank selama periode 2015-2020.
2. Mengetahui tipologi dari kasus-kasus TPPU, TPPT, dan PPSPM yang melibatkan PJP Lembaga Selain Bank dan KUPVA Bukan Bank yang sudah diputus pengadilan selama periode 2015-2020.

BAGIAN 2

TINJAUAN PUSTAKA

2.1 Kontruksi TPPU, TPPT, dan PPSPM

2.1.1 Tahapan TPPU

Pencucian uang merupakan suatu tindakan yang dilakukan untuk menyembunyikan ataupun menyamarkan dana dari hasil tindak pidana sebagaimana diatur dalam Pasal 2 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, dengan tujuan untuk menyembunyikan ataupun menyamarkan asal-usul harta kekayaan sehingga seolah-olah berasal dari sumber yang sah. Pencucian uang pada umumnya dilakukan melalui 3 (tiga) tahap, diantaranya yaitu:

1. **Penempatan (*Placement*)**

   Merupakan upaya menempatkan dana yang berasal dari hasil tindak pidana ke dalam sistem keuangan atau lembaga yang terkait dengan keuangan. Tahap penempatan merupakan tahap pertama dalam proses pemisahan harta kekayaan hasil tindak pidana dari sumber tindak pidananya.

2. **Pemisahan/Pelapisan (*Layering*)**

   Merupakan upaya memisahkan hasil tindak pidana dari sumbernya melalui beberapa tahap transaksi keuangan untuk menyembunyikan atau menyamarkan asal-usul dana. Dalam kegiatan ini terdapat proses pemindahan dana dari beberapa rekening atau lokasi tertentu ke tempat lain melalui serangkaian transaksi yang kompleks dan didesain untuk menyamarkan dan menghilangkan jejak sumber dana tersebut.

3. **Penggabungan (*Integration*)**

   Merupakan upaya menggunakan harta kekayaan hasil tindak pidana yang telah ditempatkan (*placement*) dan atau dilakukan pelapisan (*layering*) yang tampak sebagai harta kekayaan yang sah dan digunakan untuk kegiatan bisnis yang halal atau membiayai kembali kegiatan kejahatannya. Tahapan integrasi ini merupakan tahapan terakhir dari operasi pencucian uang yang lengkap karena memasukkan hasil tindak pidana tersebut kembali ke dalam kegiatan ekonomi yang sah. Dengan demikian pelaku tindak pidana dapat leluasa menggunakan harta kekayaan hasil kejahatannya tanpa menimbulkan kecurigaan dari penegak hukum untuk melakukan pemeriksaan.

Meskipun demikian, dalam praktiknya pencucian uang tidak harus terdiri dari ketiga tahap tersebut.

2.1.2 Tahapan TPPT

Pendanaan terorisme merupakan segala perbuatan dalam rangka menyediakan, mengumpulkan, memberikan, atau meminjamkan dana, baik langsung maupun tidak langsung, dengan maksud untuk digunakan dan/atau yang diketahui akan digunakan untuk melakukan kegiatan terorisme, organisasi teroris, atau teroris. Adapun yang termasuk dalam TPPT diatur dalam Pasal 4 sampai dengan Pasal 6 Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme. TPPT pada umumnya memiliki beberapa tahap diantaranya yaitu:

1. **Tahap Pengumpulan Dana (*Collecting*)**

   Merupakan upaya mengumpulkan, menyediakan, dan memberikan dana untuk melakukan tindak pidana terorisme, organisasi terorisme, atau teroris. Tahap pengumpulan dana ini dapat dilakukan dengan berbagai cara, diantaranya yaitu:

a. Donasi kepada Kelompok Teror

Donasi kepada kelompok teror ini dapat dilakukan oleh para anggota yang tidak berkaitan langsung dengan kelompok teror, diberikan secara langsung dan tunai kepada kelompok teror dalam jumlah yang kecil, atau dilakukan dengan kedok sebagai amal untuk menarik simpatisan di luar kelompok teror. Adapun dana ini sebagian besar berasal dari hasil yang legal.

b. Pendanaan Sendiri *(Self-Funding)*

Sumber dana berasal dari hasil usaha, pendapatan, dan hasil penjualan harta milik para anggota kelompok teror. *E-commerce* juga rentan digunakan oleh para anggota dan simpatisan kelompok teror untuk melakukan kegiatan usaha secara *online*. Pada pendanaan sendiri, sebagian besar dana diperoleh dalam bentuk uang tunai.

c. Pendanaan Melalui Media Sosial

Perkembangan media sosial dan mudahnya pembuatan akun media sosial memungkinkan pemanfaatan media sosial untuk menyebarkan pesan pengumpulan dana kepada masyarakat di dalam dan luar negeri. Adapun penggunaan media sosial untuk pengumpulan dana dapat berafiliasi dengan *Non Profit Organization* (NPO) tertentu dan cenderung ditujukan ke rekening pribadi pelaku. Penggunaan media sosial terenkripsi telah terbukti digunakan untuk menyampaikan pesan untuk melakukan serangan, rekrutmen, pengumpulan dana, dan kegiatan operasional lainnya.

2. Tahap Pemindahan Dana (*Moving*)

Merupakan upaya memindahkan dana yang sebelumnya telah dikumpulkan. Tahap pemindahan dana ini dapat dilakukan dengan berbagai cara, diantaranya yaitu:

a. Pembawaan Uang Tunai

Transaksi tunai masih tergolong tinggi digunakan untuk aksi pendanaan terorisme karena tidak memiliki jejak kepemilikan dan sulitnya pengecekan terhadap pembawaan uang tunai. Uang tunai dalam praktik terorisme ini seringkali digunakan dalam aksi pemberian donasi. Selain itu, uang tunai mudah dibawa ke dalam dan luar negeri, serta ditukarkan ke mata uang lainnya dalam rangka memenuhi kebutuhan aksi terorisme. Penggunaan uang tunai juga mempersulit analisis aliran dana.

b. Penggunaan PTD Berizin Selain Bank

Penggunaan PTD Selain Bank untuk memindahkan dana terorisme tergolong berisiko tinggi. Hal ini karena layanannya mudah, cepat, serta jangkauannya luas hingga ke daerah terpencil dan di berbagai belahan dunia. Penggunaan PTD Berizin Selain Bank untuk pendanaan aksi terorisme dilakukan oleh pihak-pihak yang namanya tidak tercantum dalam daftar terduga teroris. Hal ini mempersulit proses identifikasi transaksi.

c. Penggunaan Layanan Perbankan

Layanan perbankan digunakan dalam aksi terorisme karena jangkauannya yang luas sampai ke daerah terpencil dan produk yang beragam. Rekening tabungan merupakan produk yang paling banyak digunakan karena dapat digunakan untuk menampung dan memindahkan dana. Dalam rangka menghindari Aparat Penegak Hukum, pelaku seringkali menggunakan rekening keluarga, rekening pihak ketiga, rekening pinjaman, ataupun rekening yang dibeli untuk bertransaksi. Selain itu, pelaku pendanaan terorisme juga menggunakan layanan perbankan karena transaksi yang dilakukan relatif kecil dan sumber dana berasal dari hasil yang legal.

3. Tahap Penggunaan Dana (*Using*)

Merupakan upaya menggunakan dana yang sebelumnya telah dikumpulkan baik seluruhnya atau sebagian untuk mendukung pelaksanaan tindak pidana terorisme, organisasi terorisme, atau teroris. Tahap ini dapat dilakukan dengan berbagai cara diantaranya yaitu:

a. Pembelian Senjata dan Bahan Peledak

Dalam rangka melancarkan aksinya, para pelaku teror membutuhkan senjata dan bahan peledak. Dalam hal ini, pengadaan senjata dilakukan dengan membeli senjata di dalam dan luar negeri melalui penjual gelap, atau dengan merakit senjata tersebut. Senjata yang dibeli di luar negeri akan diselundupkan masuk ke wilayah Indonesia melalui jalur perbatasan yang tidak resmi. Selain itu, pembelian bahan-bahan peledak juga dilakukan melalui toko kimia baik secara langsung maupun *online*, yang dilakukan secara bertahap. Adapun risiko pembuatan bahan peledak ini dapat terjadi karena kurangnya pembatasan dan pengawasan pembelian bahan-bahan kimia.

b. Mobilitas Anggota Teror dan Perjalanan *Foreign Terrorist Fighter* (FTF)

Dalam mendukung aksi terorisme, dibutuhkan dana untuk mobilitas dari suatu tempat ke tempat lainnya. Biaya untuk mobilitas dapat bersumber dari pendanaan sendiri ataupun berasal dari anggota kelompok jaringan terorisme. Penggunaan dana untuk mobilitas anggota kelompok teror sebagian besar untuk memberangkatkan anggota untuk menjadi pejuang teroris asing. Pada umumnya, dana tersebut digunakan untuk membeli tiket transportasi dari atau ke negara konflik, serta untuk mengurus dokumen perjalanan.

c. Pelatihan Perang

Dalam rangka mendukung kegiatan aksi terorisme, dibutuhkan pelatihan terhadap fisik, mental, dan taktik bagi para pelaku teror. Dalam hal ini, dana yang bersumber dari pendanaan sendiri, ataupun sumber lainnya, akan digunakan untuk membiayai kegiatan pelatihan perang. Pelatihan perang secara fisik dibutuhkan untuk dapat mengembangkan dan meningkatkan kemampuan taktik perang, baik dalam melakukan serangan maupun untuk menyelamatkan diri. Pelatihan perang ini umumnya dilakukan secara tersembunyi dan di tempat tertutup, sehingga sulit dijangkau oleh Aparat Penegak Hukum dan masyarakat.

2.1.3 Tahapan PPSPM

PPSPM merupakan tindakan menyediakan dana dengan maksud untuk digunakan seluruhnya atau sebagian untuk manufaktur, akuisisi, kepemilikan, pengembangan, ekspor, perantara, pengangkutan, pemindahan, penimbunan atau penggunaan senjata nuklir, bahan kimia, atau senjata biologis serta sarana dan materi terkait yang bertentangan dengan hukum nasional atau ketentuan hukum internasional. Pada umumnya, tahapan PPSPM terdiri atas 3 (tiga) tahap yaitu:

a. Pengumpulan Dana (*Fund Raising*)

Merupakan upaya pengumpulan dana melalui anggaran domestik, yang dapat juga dilengkapi dengan pengumpulan dana yang dilakukan oleh jaringan di luar negeri atau oleh aktivitas kriminal.

b. Menyamarkan Dana (*Disguising the Funds*)

Merupakan upaya memindahkan dan ke sistem keuangan internasional, yang seringkali melibatkan transaksi internasional untuk tujuan perdagangan.

c. Pengadaan Bahan dan Teknologi (*Procurement*)

Merupakan upaya menggunakan dana dalam sistem keuangan internasional untuk pengadaan bahan dan teknologi yang dibutuhkan untuk melaksanakan program proliferasi dan senjata pemusnah massal.

2.2 Jenis TPPU, TPPT dan PPSPM

2.2.1 Jenis-Jenis TPPU

Pada umumnya, TPPU dapat dikategorikan menjadi beberapa jenis. Berdasarkan penyusunan dakwaannya, TPPU disebut sebagai *Stand-Alone Money Laundering*. Disebut demikian karena TPPU pada dasarnya merupakan tindak pidana lanjutan dari suatu tindak pidana asal. Namun, TPPU ini diartikan sebagai tindak pidana yang berdiri sendiri dengan mengacu pada penuntutan tindak pidana pencucian uang secara tunggal, tanpa harus menuntut tindak pidana asal. Dalam hal ini, penyusunan dakwaan TPPU dapat dijadikan satu berkas dengan tindak pidana asalnya ataupun dipisah dengan tindak pidana asalnya. Hal ini dianggap relevan karena:

1. Terdapat kemungkinan tidak adanya cukup bukti dari tindak pidana asal tertentu yang menimbulkan hasil kejahatan; atau
2. Dalam situasi dimana terdapat kekurangan pada wilayah hukum atas terjadinya tindak pidana asal. Harta kekayaan yang diperoleh dari tindak pidana kemungkinan telah dicuci oleh terdakwa (*self-laundering*) atau oleh pihak ketiga (*third party money laundering*).

Lebih lanjut, berdasarkan hubungan dengan pelaku tindak pidana asal, TPPU dapat dikategorikan sebagai berikut:

1. *Self-Laundering*, yaitu pencucian uang yang dilakukan oleh orang yang terlibat dalam perbuatan tindak pidana asal.
2. *Third Party Money Laundering*, yaitu pencucian uang yang dilakukan oleh orang yang tidak terlibat dalam perbuatan tindak pidana asal.

Sementara itu, berdasarkan tempat terjadinya, terdapat TPPU yang dikenal dengan istilah *Foreign Money Laundering*. *Foreign Money Laundering* ini merupakan pencucian uang yang dilakukan di luar yurisdiksi dari tempat terjadinya tindak pidana asal. Hal ini dilakukan untuk menyulitkan Aparat Penegak Hukum dalam menelusuri hasil tindak pidana. Di Indonesisa, TPPU telah diatur dalam Undang-Undang No.8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Dalam UU ini, TPPU dibedakan menjadi:

a. Tindak Pidana Pencucian Uang Aktif

TPPU aktif merupakan jenis pencucian uang dimana adanya perbuatan aktif untuk menyembunyikan dan menyamarkan harta kekayaan hasil tindak pidana. Ketentuan mengenai TPPU aktif diatur dalam Pasal 3 dan Pasal 4 UU TPPU.

b. Tindak Pidana Pencucian Pasif

TPPU pasif merupakan jenis pencucian uang dimana tidak adanya perbuatan aktif untuk menyembunyikan dan menyamarkan harta kekayaan hasil tindak pidana. Ketentuan mengenai TPPU pasif diatur dalam Pasal 5 ayat (1) UU TPPU.

2.2.2 Jenis-Jenis TPPT

Pada dasarnya praktik TPPT terdiri atas beberapa kategori, diantaranya:

1. Pengumpulan Dana—Legal: Sponsor Pribadi (*Terrorist Financier/Fundraiser*)

Pengumpulan dana yang dilakukan secara legal dengan melakukan kegiatan penggalangan dana melalui sponsor.

2. Pengumpulan Dana—Legal: Penyimpangan Pengumpulan Donasi Melalui Ormas

Pengumpulan dana yang dilakukan secara legal dengan melakukan kegiatan pengumpulan donasi melalui organisasi kemasyarakatan (ormas).

3. **Pengumpulan Dana—Legal: Usaha Bisnis yang Sah**

   Pengumpulan dana yang dilakukan secara legal dengan membentuk suatu perusahaan atau bisnis yang sah yang dijadikan sebagai media untuk mengumpulkan dana.

4. **Pengumpulan Dana—Legal: Pendanaan *Crowdfunding***

   Pengumpulan dana yang dilakukan secara legal dengan memanfaatkan *financial technology*, yaitu melalui pendanaan *crowdfunding*.

5. **Pengumpulan Dana—Legal: Pendanaan Mandiri (Selain dari Usaha Bisnis)**

   Pengumpulan dana yang dilakukan secara legal yaitu dengan melakukan kegiatan penggalangan dana atau pendanaan yang dilaksanakan secara mandiri.

6. **Pengumpulan Dana—Ilegal: Hasil Kegiatan Kriminal Lainnya**

   Pengumpulan dana yang dilakukan secara ilegal yaitu dengan memperoleh dana melalui hasil tindakan kriminal.

7. **Pengumpulan Dana—Ilegal: Pemerasan**

   Pengumpulan dana yang dilakukan secara ilegal yaitu dengan melakukan pemerasan kepada pihak tertentu untuk memperoleh dana.

8. **Pengumpulan Dana—Ilegal: Eksploitasi Sumber Daya Alam Secara Ilegal**

   Pengumpulan dana yang dilakukan secara ilegal yaitu dengan melakukan kegiatan eksploitasi sumber daya alam secara melawan hukum.

9. **Pengumpulan Dana—ilegal: Penculikan dengan Tebusan**

   Pengumpulan dana yang dilakukan secara ilegal yaitu melakukan penculikan dengan disertai tindakan meminta tebusan, dimana dana tebusan akan dikumpulkan untuk pendanaan kegiatan terorisme.

10. **Pemindahan Dana: Melalui Penyedia Jasa Keuangan**

    Dana yang telah dikumpulkan dipindahkan dengan menggunakan layanan jasa keuangan.

11. **Pemindahan Dana: Melalui Pembawaan Uang Tunai Lintas Batas**

    Dana yang telah dikumpulkan dipindahkan melalui tindakan pembawaan uang tunai lintas batas negara.

12. **Pemindahan Dana: Menggunakan Metode Pembayaran Baru**

    Dana yang telah dikumpulkan dipindahkan melalui metode pembayaran baru.

13. **Pemindahan Dana: Melalui Penyedia Barang dan Jasa**

    Dana yang telah dikumpulkan dipindahkan dengan memanfaatkan layanan penyedia barang dan jasa.

14. **Pemindahan Dana: Melalui Profesi**

    Dana yang telah dikumpulkan dipindahkan dengan memanfaatkan profesi tertentu.

15. **Penggunaan Dana: Operasi Terorisme Domestik—Pembelian Senjata dan Bahan Peledak**

    Dana digunakan untuk kegiatan terorisme yang bersifat domestik, dengan membeli senjata dan bahan peledak.

16. **Penggunaan Dana: Pelatihan—Pembuatan Senjata dan Bahan Peledak**

    Dana digunakan untuk membiayai kegiatan pelatihan, berupa pembuatan senjata dan bahan peledak.

17. **Penggunaan Dana: Pelatihan—Penggunaan Senjata dan Bahan Peledak**

    Dana digunakan untuk membiayai kegiatan pelatihan, yaitu untuk penggunaan senjata dan bahan peledak.

18. **Penggunaan Dana: Operasi Terorisme Domestik—Perjalanan dari dan ke Lokasi Aksi Terorisme**

    Dana digunakan untuk membiayai kegiatan terorisme dalam lingkup domestik, yaitu untuk perjalanan dari dan ke lokasi aksi terorisme.

19. **Penggunaan Dana: Operasi Terorisme Luar Negeri—Perjalanan Pejuang Teroris Asing**

    Dana digunakan untuk membiayai kegiatan terorisme di luar negeri, yaitu untuk perjalanan pejuang teroris asing.

20. **Penggunaan Dana: Gaji dan Kompensasi Anggota Kelompok Terorisme—Santunan kepada Anggota yang Masuk Penjara atau Meninggal**

    Dana digunakan untuk membiayai operasional kelompok terorisme, seperti untuk membayar gaji dan kompensasi, serta untuk memberikan santunan kepada anggota kelompok yang masuk penjara atau meninggal.

21. **Penggunaan Dana: Gaji dan Kompensasi Anggota Kelompok**

    Dana digunakan untuk membiayai operasional kelompok terorisme yaitu untuk membayar gaji dan kompensasi kepada anggota kelompok.

22. **Penggunaan Dana: Operasi Terorisme Domestik—Biaya Hidup Dasar (Pangan, Papan, Biaya Medis)**

    Dana digunakan untuk kegiatan terorisme dalam lingkup domestik, yaitu untuk membiayai kebutuhan dasar hidup sehari-hari, seperti pangan, papan, dan biaya medis.

23. **Penggunaan Dana: Propaganda dan Perekrutan—Pembuatan dan Pemeliharaan Akun di Media Sosial**

    Dana digunakan untuk membiayai aktivitas propaganda dan perekrutan anggota, yaitu untuk pembuatan dan pemeliharaan akun di media sosial.

24. **Penggunaan Dana: Pelatihan—Ideologi**

    Dana digunakan untuk kegiatan pelatihan, yaitu untuk kegiatan menanamkan ideologi kelompok terorisme.

25. **Penggunaan Dana: Operasi Terorisme Domestik—Dokumen Identitas Palsu**

    Dana digunakan untuk kegiatan terorisme dalam lingkup domestik, yaitu berupa pembuatan dokumen identitas palsu.

26. **Penggunaan Dana—Propaganda dan Perekrutan—Pembuatan dan Pemeliharaan Situs Web**

    Dana digunakan untuk kegiatan propaganda dan perekrutan anggota kelompok terorisme, yaitu berupa kegiatan pembuatan dan pemeliharaan situs web.

27. **Penggunaan Dana: Pelatihan—Pelatihan *Virtual/Online***

    Dana digunakan untuk kegiatan pelatihan anggota kelompok terorisme yang dilakukan secara *virtual/online*.

28. **Penggunaan Dana: Operasi Terorisme Domestik—Pembelian dan Perawatan Kendaraan atau Mesin**

    Dana digunakan untuk kegiatan terorisme dalam lingkup domestik, yaitu berupa pembelian dan perawatan kendaraan atau mesin yang digunakan dalam aksi terorisme.

29. **Penggunaan Dana: Biaya Kurir (Pengiriman Pesan, Uang)**

    Dana digunakan untuk biaya kurir dalam kegiatan pengiriman pesan atau uang.

30. **Penggunaan Dana: Pelatihan Komunikasi Rahasia/Sandi**

    Dana digunakan untuk membiayai kegiatan pelatihan komunikasi rahasia/sandi bagi kelompok terorisme.

31. **Penggunaan Dana: Propaganda dan Perekrutan—Pembuatan Majalah/Koran**

    Dana digunakan untuk kegiatan propaganda dan perekrutan anggota kelompok terorisme, yaitu berupa pembuatan majalah/koran.

32. **Penggunaan Dana: Propaganda dan Perekrutan—Media Promosi Lainnya (Televisi, Radio)**

    Dana digunakan untuk kegiatan propaganda dan perekrutan anggota kelompok terorisme yaitu berupa pembiayaan media promosi seperti televisi dan radio.

33. **Penggunaan Dana: Pelatihan—Pembangunan Lokasi Pelatihan**

    Dana digunakan untuk kegiatan pelatihan, yaitu dalam rangka membiayai pembangunan lokasi pelatihan.

2.2.3 Jenis-Jenis PPSPM

Pada umumnya PPSPM memiliki karakteristik sebagai berikut:

1. Beroperasi secara global dan mengeksploitasi negara-negara dengan kontrol ekspor dan keuangan yang lemah.
2. Penggunaan sistem keuangan formal, namun juga memungkinkan penggunaan sarana informal dan uang tunai.
3. Pembelian barang sensitif proliferasi melalui pasar terbuka.
4. Penggunaan perusahaan cangkang *(shell company)* dan perantara perdagangan untuk menyamarkan penggunaan akhir dan pengguna akhir pengadaan yang sebenarnya.

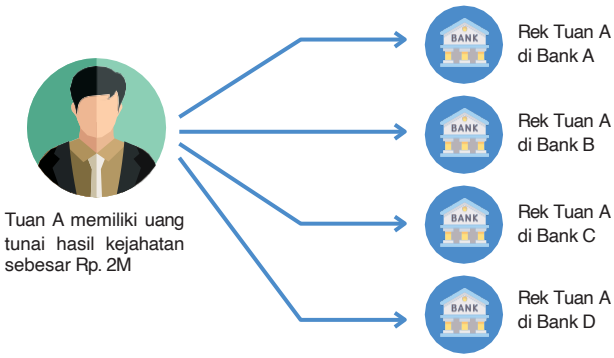
2.3 Skema Tipologi TPPU, TPPT, dan PPSPM

Adapun beberapa contoh skema tipologi TPPU, TPPT, dan PPSPM dapat dilihat pada bagan berikut:

1. Skema *Smurfing*

Smurfing merupakan transaksi yang dilakukan dengan menggunakan beberapa rekening atas nama individu yang berbeda-beda.

Gambar 2.1. Skema *Smurfing*

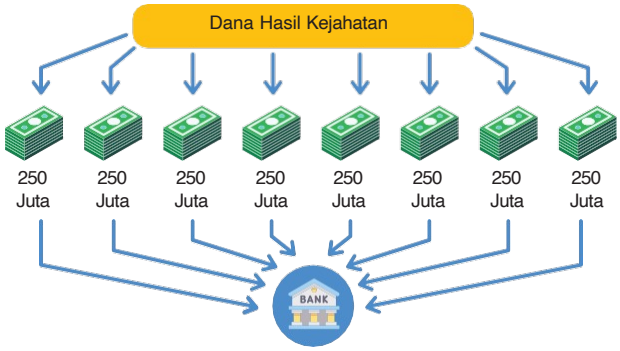


Sumber: PPATK

2. Skema *Structuring*

Structuring merupakan aktivitas memecah-mecah transaksi, dimana transaksi dalam jumlah yang relatif kecil namun dilakukan dalam beberapa tahap dengan frekuensi yang tinggi dalam periode waktu tertentu.

Gambar 2.2. Skema *Structuring*

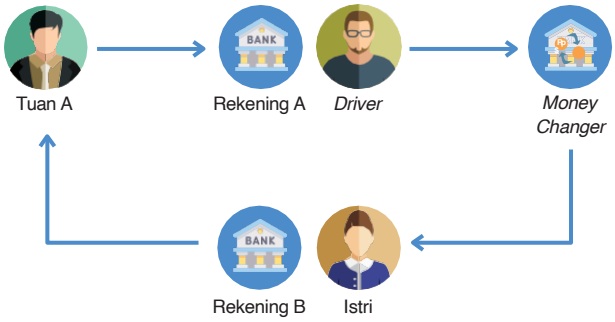


Sumber: PPATK

3. Skema Transaksi *U-Turn*

Transaksi U-*Turn* merupakan transaksi yang dilakukan secara berputar balik, dimana dana ditransfer ke rekening lain dan pada akhirnya akan dilakukan transfer kembali ke rekening asal demi menyamarkan asal-usul hasil kejahatan tersebut.

Gambar 2.3. Skema Transaksi *U-Turn*

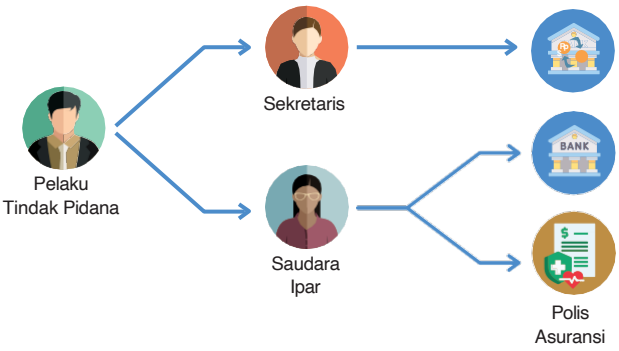


Sumber: PPATK

4. Skema Penggunaan Pihak Ketiga

Penggunaan pihak ketiga merupakan transaksi yang dilakukan dengan menggunakan identitas orang lain (pihak ketiga) ataupun dengan menggunakan rekening pihak ketiga yang bertujuan untuk menyembunyikan dan menyamarkan identitas dari pihak sebenarnya yang memiliki dana hasil kejahatan.

Gambar 2.4. Skema Penggunaan Pihak Ketiga

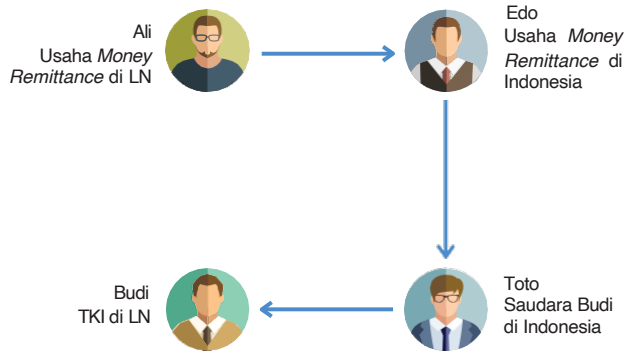


Sumber: PPATK

5. Skema Penggunaan Jasa Informal Transfer

Penggunaan jasa informal transfer merupakan transaksi pengiriman uang yang dilakukan dengan menggunakan jasa pengiriman uang di luar jasa keuangan resmi seperti bank, yang dilakukan atas dasar kepercayaan.

Gambar 2.5. Skema Penggunaan Jasa Informal Transfer

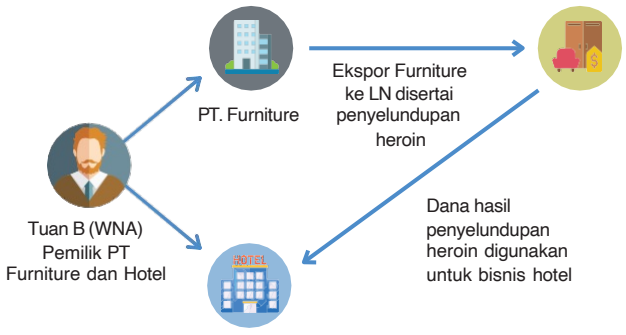


Sumber: PPATK

6. Skema Penggunaan Perusahaan Legal

Penggunaan perusahaan legal merupakan aktivitas transaksi yang melibatkan suatu perusahaan dengan usaha yang sah dengan tujuan untuk menyamarkan aktivitas keuangan ilegal yang berasal dari suatu kejahatan.

Gambar 2.6. Skema Penggunaan Perusahaan Legal

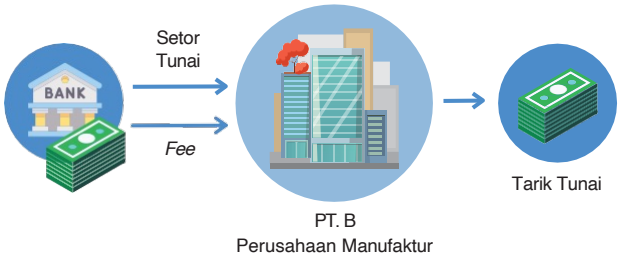


Sumber: PPATK

7. Skema Transaksi Perusahaan yang Tidak Sesuai dengan Jenis Usahanya

Transaksi perusahaan yang tidak sesuai dengan jenis usahanya merupakan transaksi dari perusahaan yang terdaftar dengan bidang usaha tertentu, misalnya manufaktur, dan tidak memiliki izin usaha untuk melakukan pengiriman uang, akan tetapi melakukan kegiatan pengiriman uang.

Gambar 2.7. Skema Transaksi Perusahaan yang Tidak Sesuai dengan Jenis Usahanya



Sumber: PPATK

2.4 Tipologi Berdasarkan Tindak Pidana Asal (TPA)

2.4.1 Penipuan Siber

A. Jenis/Karakteristik Penipuan Siber

Merujuk pada SRA TPPU pada TP Penipuan Siber (2022), beberapa jenis/karakteristik penipuan siber sebagai berikut:

1. *Business Email Compromise* (BEC)
   Pelaku kejahatan meretas sistem *email* untuk mendapatkan informasi tentang mekanisme pembayaran perusahaan, kemudian menipu karyawan perusahaan untuk mentransfer uang ke rekening pelaku kejahatan.

2. *Fraudulent Wire Transfer*
   Korban secara acak dihubungi oleh pelaku kejahatan yang mengaku sebagai teman, kerabat, wakil perusahaan atau pihak berwenang lainnya sehingga korban secara sukarela (seringkali melibatkan emosi) mengirimkan uang kepada pelaku.

3. *Investment Fraud*
   Korban dibujuk untuk berinvestasi dalam saham palsu atau investasi lainnya dengan iming-iming keuntungan yang besar namun sebenarnya tidak menguntungkan atau tidak ada kegiatan investasi.

4. *Romance Scam*
   Penjahat menjalin "hubungan khusus" dengan korban biasanya melalui media sosial dengan tujuan akhir mendapatkan uang dari korban.

B. Tipologi TPPU dan TPPT pada Penipuan Siber

1. Penggunaan dokumen identitas palsu.

2. Pembuatan rekening baru untuk menampung dana hasil kejahatan.

3. Penggunaan rekening *nominee*, milik orang lain baik yang dikenal atau tidak kenal/fiktif.

4. Pola transaksi menggunakan uang tunai, yaitu tarik atau setor tunai yang dilakukan untuk menyamarkan identitas.

5. Transaksi yang dilakukan secara *pass by* (dana masuk langsung ditransfer kembali atau Tarik tunai).

6. Penggunaan nama perusahaan atau perseorangan untuk menampung pengiriman uang sehingga seolah-olah tampak seperti transaksi bisnis.

C. Produk/Jasa yang Disalahgunakan untuk Penipuan Siber

1. Transfer dana, baik domestik maupun *cross border;*

2. Tabungan;

3. Kartu debit, uang elektronik;

4. Tarik/setor tunai.

2.4.2 Bidang Perpajakan

Merujuk pada Surat Edaran PPATK tentang Indikator TKM terkait TP di Bidang Perpajakan (2021), beberapa tipologi di bidang perpajakan sebagai berikut:

A. Transaksi yang Menyimpang dari Profil, Karakteristik atau Kebiasaan Pola Transaksi Pengguna Jasa yang Bersangkutan:

1. Rekening pribadi, khususnya dengan profil swasta, digunakan untuk transaksi bisnis/menampung hasil penjualan dalam jumlah signifikan.

2. Rekening pribadi yang menerima pengalihan dana bersumber dari hasil perjudian di luar negeri.

3. Rekening pribadi pengurus/anggota keluarga pengurus/karyawan perusahaan menerima dana dalam jumlah signifikan dan/atau rutin dari perusahaan tempat yang bersangkutan bekerja, dan/atau dari pihak-pihak yang memiliki kesamaan profil usaha dengan perusahaan tempat yang bersangkutan bekerja, misalnya penggunaan rekening pribadi untuk pembayaran hasil ekspor, penggunaan rekening pribadi untuk menjadi rekening penampung pembayaran mesin EDC milik perusahaan.

4. Peningkatan volume transaksi dari rata-rata transaksi sebelumnya, dengan indikator sebagai berikut:

    a. Peningkatan volume transaksi per tahun (lebih dari 3 kali lipat) dari volume transaksi tahun sebelumnya; dan/atau
    b. Peningkatan nilai transaksi (lebih dari 3 kali lipat) dari rata-rata transaksi sebelumnya, misalnya peningkatan signifikan setoran tunai ke rekening pihak yang melakukan transaksi keuangan dimana pihak tersebut biasanya menerima pembayaran non tunai.

5. Transaksi keuangan yang dilakukan jauh melebihi kemampuan bertransaksi/ bisnis/indikator lainnya yang dinyatakan dalam formulir pembukaan rekening.

6. Transaksi keuangan tidak konsisten dengan profil pemilik rekening, misalnya, rekening individu bertransaksi dengan rekening perusahaan dalam frekuensi tinggi.

7. Transaksi keuangan terkait instruksi pembayaran dengan mutasi transaksi keuangan yang melibatkan banyak pihak (*layering*) dan cenderung berbeda dari praktek bisnis pada umumnya atau menyimpang dari kelaziman suatu industri beroperasi, misalnya ketidaklaziman antara lain penggunaan transaksi tunai pada perdagangan internasional dan *e-commerce.*

8. Transaksi pembayaran remunerasi dalam jumlah signifikan dan biasanya dibayarkan untuk jenis layanan tertentu.

9. Pengguna jasa melakukan transaksi dengan tidak memperhatikan keuntungan/ kerugiannya, misalnya mengabaikan tingkat keuntungan dari komisi yang lebih tinggi, suku bunga yang lebih tinggi dan lain sebagainya.

10. Transaksi keuangan dalam jumlah signifikan dilakukan pada rekening yang baru dibuka enam bulan sebelumnya.

11. Rekening perseorangan dengan profil pekerjaan swasta/ wiraswasta melakukan transaksi yang mencantumkan berita transaksi berkaitan dengan pajak, antara lain "PPN", bayar pajak, konsultasi pajak, faktur, dan sebagainya.

12. Rekening perorangan dengan profil swasta, misalnya profil Direktur, pemilik perusahaan, atau pegawai swasta melakukan transaksi yang diantaranya mencantumkan berita transaksi yang diduga terkait dengan operasional/bisnis perusahaan, antara lain operasional, pembayaran, dan pembayaran faktur, *supplier*, dan sebagainya.

13. Terdapat transaksi rutin dengan pihak yang memiliki profil usaha serupa dengan wajib pajak.

14. Terdapat transaksi atau setoran awal rekening perusahaan melebihi modal disetor yang tercantum dalam akta notaris pendirian perusahaan.

15. Nilai jaminan atas kredit yang diajukan jauh melebihi modal disetor yang tercantum dalam akta notaris pendirian perusahaan.

16. Pembayaran dividen lebih dari 1 (satu) kali dalam periode yang sama.

17. Penggunaan bisnis usaha yang menggunakan transaksi tunai secara intensif.

18. Adanya transaksi yang signifikan dengan pihak terafiliasi, transaksi seperti ini diduga merupakan modus *transfer pricing* untuk mengecilkan beban pajak salah satu perusahaan afiliasi.

19. Transaksi yang berbeda jauh dengan periode sebelumnya yang berpotensi adanya biaya fiktif.

20. Perusahaan termasuk dalam kawasan berikat, tetapi banyak melakukan transaksi penjualan atau menerima dana dengan pihak dalam negeri.

21. Perusahaan/orang pribadi menerima dana dalam jumlah signifikan tanpa ada *underlying transaction* yang jelas dari luar negeri. Hal ini berpotensi wajib pajak tidak membayarkan PPh.

22. Perusahaan yang menjual barang ekspor namun dalam rekeningnya tidak pernah atau jarang menerima pembayaran dari luar negeri.

23. Pengguna jasa melakukan transaksi keuangan yang cukup signifikan di luar informasi yang disampaikan pada profil pembukaan rekening, tanpa disertai informasi mengenai Nomor Pokok Wajib Pajak (NPWP) yang bersangkutan.

24. Transaksi *U-turn* dalam dengan pihak yang sama dan/atau pihak terafiliasi, di luar negeri, terutama dengan negara yang memiliki tingkat pajak lebih rendah dari Indonesia sebagaimana daftar *Corporate Tax Haven Index*, dan transaksi ini dilakukan secara berulang-ulang.

25. Penerbitan obligasi dimana pembelinya adalah perusahaan terafiliasi yang terdaftar dari *tax haven country*.

26. Pengguna Jasa membeli kendaraan yang masuk dalam kategori barang sangat mewah dan/atau barang dengan nilai satuan/kumulatif lebih dari Rp1.000.000.000,00 (satu miliar rupiah) dengan menggunakan nama orang lain guna menghindari PPh atau menghindari pajak progresif. Terdapat transaksi keuangan Pengguna Jasa dengan tujuan transaksi pembelian properti yang jumlahnya lebih tinggi dari akta jual beli.

27. Terdapat pengiriman dana dengan jumlah signifikan dari rekening perusahaan ke pihak ketiga di luar struktur pengurus/pemilik perusahaan. Terutama bila pengiriman dana dilakukan pada saat usaha/perusahaan ingin melaporkan saldonya di akhir bulan Desember atau tahun pajak.

28. Terdapat pemindahan dana dengan jumlah signifikan ke pihak yang sama dan/atau pihak yang terafiliasi dengan perlakukan pajak khusus seperti rekening Yayasan, LSM, NPO, Mahasiswa dan Pensiunan.

29. Pemanfaatan rekening atas nama anggota keluarga atau rekening dengan jenis rekening pribadi yang digunakan oleh entitas bisnis untuk menerima atau mengelola dana dari hasil usaha dengan nilai yang signifikan, untuk menerima dana dari hasil usaha, dengan pola transaksi penarikan tunai dan penyetoran tunai dimana transaksi tersebut sebenarnya bisa dilakukan dengan transaksi pemindahbukuan.

B. Transaksi yang Patut Diduga Dilakukan dengan Tujuan untuk Menghindari Pelaporan Transaksi yang Bersangkutan yang Wajib Dilakukan oleh Penyedia Jasa Keuangan (PJK) Sesuai Ketentuan UU TPPU:

Transaksi pengalihan dana dalam jumlah kecil dan sering serta dalam waktu yang berdekatan dengan jumlah signifikan dan/atau rutin dari rekening perusahaan ke rekening individu yang tercatat sebagai pengurus/karyawan/pemilik/ pemegang saham, dengan pola penarikan tunai dan penyetoran tunai yang seharusnya merupakan transaksi pemindahbukuan.

C. Transaksi yang Dilakukan atau Batal Dilakukan dengan Menggunakan Harta Kekayaan yang Diduga Berasal dari Hasil Tindak Pidana:

1. Terdapat dugaan pemalsuan identitas seperti penggunaan NPWP dan Kartu Tanda Penduduk (KTP) fiktif.

2. Transaksi maupun saldo rekening dalam jumlah signifikan milik pihak yang namanya tercantum dalam *open sources*[1] yang dapat dipertanggungjawabkan kebenarannya.

D. Transaksi yang Diminta oleh PPATK untuk Dilaporkan oleh PJK[2] karena Melibatkan Harta Kekayaan yang Diduga Berasal dari Hasil Tindak Pidana:

1. Transaksi Keuangan yang diminta oleh PPATK karena Pengguna Jasa telah ditetapkan sebagai tersangka/terdakwa dalam kasus tindak pidana di bidang perpajakan.

2. Transaksi Keuangan oleh Pengguna Jasa yang diminta oleh PPATK karena keterkaitannya dengan Transaksi lain terkait tindak pidana di bidang perpajakan yang sedang dalam proses analisis maupun pemeriksaan oleh PPATK.

3. Transaksi Keuangan oleh Pengguna Jasa yang diminta oleh PPATK atas dasar penyelidikan atau penyidikan terkait tindak pidana di bidang perpajakan yang sedang dilakukan oleh aparat penegak hukum.

2.4.3 Kepabeaan dan Cukai

Merujuk pada SRA TBML (2021), terdapat beberapa tipologi dan indikator transaksi keuangan mencurigakan indikasi TPPU berbasis perdagangan sebagai berikut:

A. Indikator Struktural

1. Struktur perusahaan dari entitas perdagangan tampak sangat kompleks dan tidak logis, seperti keterlibatan perusahaan cangkang atau perusahaan yang terdaftar di yurisdiksi berisiko tinggi.

2. Entitas perdagangan terdaftar atau memiliki kantor di yurisdiksi dengan tingkat kepatuhan APU PPT yang tidak memadai atau lemah.

3. Entitas perdagangan terdaftar di alamat berupa alamat pendaftaran massal, misalnya bangunan tempat tinggal dengan kepadatan tinggi, alamat kotak pos, bangunan komersial atau kompleks industri, terutama ketika tidak ada referensi ke unit tertentu.

4. Kegiatan usaha entitas perdagangan tidak sesuai dengan alamat yang dicantumkan, misalnya entitas perdagangan tampaknya menggunakan properti tempat tinggal, tanpa memiliki ruang komersial atau industri, tanpa penjelasan yang masuk akal.

---

[1] *Open sources* berupa daftar nama yang terlibat kegiatan ilegal (*tax evasion*).

[2] PJK sesuai Pasal 17 UU No. 18 Tahun 2010 tentang Pencegahan dan Pemberantasan TPPU yang mencakup PJP dan KUPVA BB.

5. Entitas perdagangan tidak memiliki kanal *online* atau kanal *online* menunjukkan aktivitas bisnis yang tidak konsisten dengan lini bisnis yang didaftarkan resmi, misalnya situs web entitas perdagangan sebagian besar berisi materi *boilerplate* yang diambil dari situs web lain atau situs web menunjukkan kurangnya pengetahuan mengenai produk atau industri tertentu yang ditawarkan.

6. Entitas perdagangan menunjukkan kurangnya aktivitas bisnis selayaknya perusahaan, misalnya tidak memiliki transaksi penggajian reguler sesuai dengan jumlah karyawan yang disebutkan, transaksi yang berkaitan dengan biaya operasional, atau pembayaran pajak.

7. Pemilik atau manajer senior entitas perdagangan tampaknya merupakan calon yang bertindak untuk menyembunyikan pemilik manfaat yang sebenarnya (*Beneficial Ownership*), misalnya mereka kurang pengalaman dalam manajemen bisnis atau kurang pengetahuan tentang detil transaksi, atau mengelola banyak perusahaan.

8. Entitas perdagangan, atau pemilik atau manajer senior muncul dalam berita negatif, misalnya skema pencucian uang di masa lalu, penipuan, penghindaran pajak, kegiatan kriminal lainnya, atau investigasi atau hukuman yang sedang berlangsung atau di masa lalu.

9. Entitas perdagangan mempertahankan jumlah staf kerja yang minimal, tidak sesuai dengan volume komoditas yang diperdagangkan.

10. Nama entitas perdagangan merupakan salinan dari nama perusahaan terkenal atau sangat mirip dengannya, berpotensi dalam upaya untuk terlihat sebagai bagian dari Perusahaan tersebut, meskipun sebenarnya tidak terhubung dengannya.

11. Entitas perdagangan memiliki periode dormansi yang tidak dapat dijelaskan.

12. Entitas tidak mematuhi kewajiban bisnis reguler, seperti mengajukan pengembalian PPn.

B. Indikator Aktivitas Perdagangan

1. Aktivitas perdagangan tidak konsisten dengan bidang usaha yang didaftarkan atau dideklarasikan, misalnya, pedagang mobil mengekspor pakaian atau pedagang logam mulia mengimpor makanan laut.

2. Entitas perdagangan terlibat dalam transaksi perdagangan yang kompleks yang melibatkan banyak perantara pihak ketiga dan dalam bidang usaha yang tidak sesuai.

3. Entitas perdagangan terlibat dalam transaksi dan rute atau metode pelayaran yang tidak sesuai dengan praktik bisnis standar.

4. Entitas perdagangan menggunakan produk keuangan yang tidak konvensional atau terlalu rumit, misalnya penggunaan *letter of credit* untuk jangka waktu yang sangat lama atau sering diperpanjang tanpa alasan yang jelas, terdapat pembauran berbagai jenis produk pembiayaan perdagangan untuk segmen transaksi perdagangan yang berbeda.

5. Entitas perdagangan secara konsisten menampilkan margin keuntungan yang sangat rendah dalam transaksi perdagangannya, misalnya mengimpor komoditas grosir dengan/atau di atas nilai eceran, atau menjual kembali komoditas dengan harga yang sama atau di bawah harga beli.

6. Entitas perdagangan membeli komoditas, tetapi pembelian tersebut melebihi kemampuan keuangan entitas tersebut sehingga mengandalkan pihak ketiga, misalnya transaksi dibiayai melalui masuknya setoran tunai secara tiba-tiba atau transfer pihak ketiga ke rekening entitas.

7. Entitas perdagangan yang baru dibentuk atau baru diaktifkan kembali terlibat dalam aktivitas perdagangan bervolume tinggi dan bernilai tinggi, misalnya entitas yang tidak dikenal tiba-tiba muncul dan terlibat dalam kegiatan perdagangan di sektor-sektor dengan hambatan tinggi untuk masuk pasar.

C. Indikator Aktivitas Akun dan Transaksi

1. Entitas perdagangan membuat perubahan mendekati batas waktu, misal entitas mengalihkan pembayaran ke entitas yang sebelumnya tidak dikenal pada saat terakhir, atau entitas meminta perubahan pada tanggal pembayaran terjadwal atau jumlah pembayaran.

2. Sebuah akun menampilkan jumlah atau nilai transaksi yang tinggi secara tak terduga dan tidak sesuai dengan aktivitas bisnis klien yang didaftarkan/dideklarasikan.

3. Akun entitas perdagangan diduga merupakan akun “transit” dengan pergerakan transaksi volume tinggi yang cepat dan saldo akhir hari yang kecil tanpa alasan bisnis yang jelas, termasuk:

    a. Sebuah akun sering menampilkan setoran tunai yang kemudian ditransfer ke orang atau entitas di zona perdagangan bebas atau yurisdiksi lepas pantai tanpa hubungan bisnis dengan pemegang akun.

    b. Transfer dana ke suatu akun yang terkait dengan perdagangan, kemudian dibagi dan diteruskan ke beberapa akun yang tidak terkait aktivitas komersial.

4. Pembayaran komoditas impor dilakukan oleh entitas selain penerima komoditas tanpa alasan ekonomi yang jelas, mis. oleh *shell* atau *front company* yang tidak terlibat dalam transaksi perdagangan.

5. Setoran tunai atau transaksi lain dari entitas perdagangan secara konsisten tepat di bawah ambang pelaporan yang relevan.

6. Aktivitas transaksi yang terkait dengan entitas perdagangan mengalami peningkatan volume yang cepat dan signifikan, namun kemudian menjadi tidak aktif dalam waktu singkat.

7. Pembayaran dikirim atau diterima dalam jumlah besar untuk perdagangan di sektor yang dianggap tidak biasa.

8. Transaksi *U-Turn*. Dana dikirim dari satu negara dan diterima kembali di negara yang sama, setelah melewati negara lain.

D. Indikator Dokumen dan Komoditas

1. Inkonsistensi di seluruh kontrak, faktur, atau dokumen perdagangan lainnya, misalnya kontradiksi antara nama badan pengekspor dan nama penerima pembayaran; perbedaan harga pada faktur dan kontrak yang mendasarinya; atau perbedaan antara kuantitas, kualitas, volume, atau nilai komoditas yang sebenarnya dan deskripsinya.

2. Kontrak, faktur, atau dokumen perdagangan lainnya menampilkan biaya atau harga yang tampaknya tidak sejalan dengan pertimbangan komersial, tidak konsisten dengan nilai pasar, atau

berfluktuasi secara signifikan dari transaksi sebelumnya yang sebanding.

3. Kontrak, faktur, atau dokumen perdagangan lainnya memiliki deskripsi yang tidak jelas tentang komoditas yang diperdagangkan, mis. subjek kontrak hanya dijelaskan secara umum atau non-spesifik.

4. Dokumen perdagangan atau pabean yang mendukung transaksi tidak ada, tampak palsu, menyertakan informasi yang salah atau menyesatkan, merupakan penyerahan kembali dokumen yang sebelumnya ditolak, atau sering diubah atau diubah.

5. Kontrak yang mendukung transaksi perdagangan yang kompleks atau reguler namun memiliki struktur kontrak sangat sederhana, mis. mengikuti struktur "contoh kontrak" yang tersedia di internet.

6. Nilai impor yang terdaftar dari suatu entitas menunjukkan ketidaksesuaian yang signifikan dengan volume transfer bank luar negeri untuk impor. Sebaliknya, nilai ekspor terdaftar menunjukkan ketidaksesuaian yang signifikan dengan transfer bank luar negeri yang masuk.

7. Barang-barang yang diimpor ke suatu negara selanjutnya diekspor ke negara lain dengan dokumen yang diduga palsu.

8. Pengiriman komoditas (pelayaran) melalui rute melewati sejumlah yurisdiksi (transit) tanpa pertimbangan nilai ekonomi atau komersial yang masuk akal.

2.4.4 Narkotika

Merujuk pada Surat Edaran PPATK tentang Indikator TKM terkait TP Narkotika (2019), terdapat beberapa tipologi dan indikator transaksi keuangan mencurigakan sebagai berikut:

A. Transaksi yang Menyimpang dari Profil, Karakteristik atau Kebiasaan Pola Transaksi Pengguna Jasa yang Bersangkutan:

1. Pengguna jasa melakukan transaksi dengan nilai signifikan yang tidak sesuai dengan profilnya.

2. Penarikan tunai dalam waktu yang tidak terlalu lama semenjak dilakukannya setoran tunai dalam jumlah yang signifikan.

3. Penukaran atau pembelian uang kertas asing dalam jumlah relatif besar.

4. Transaksi yang tidak sesuai profil, misalnya pihak pengirim dana ke rekening orang perseorangan memiliki profil pekerjaan antara lain pemilik warung makan, usaha ekspedisi perorangan, pelajar/mahasiswa, kepala sekolah/guru, pemilik toko pakaian *online*, *security* atau tenaga pengaman dan pengepul rongsok.

5. Transaksi pengiriman uang yang dilakukan dari atau ke negara yang terkenal sebagai tempat produksi, peredaran, dan/atau penyelundupan narkotika tanpa alasan (*underlying transaction*) yang jelas.

6. Pembelian polis asuransi yang tidak sesuai dengan profil pekerjaan dan penghasilan pengguna jasa.

7. Pengguna jasa memiliki portofolio investasi sangat besar yang tidak sesuai dengan profil pekerjaan dan penghasilan.

8. Transaksi tampak tidak sesuai dengan karakteristik, atau tidak konsisten dengan aktivitas atau kegiatan bisnis pengguna jasa.

9. *Walk in customer* melakukan transaksi transfer dana ke luar negeri dengan sumber

dana yang tidak berasal dari rekening di bank, misalnya membawa uang tunai fisik.

10. Pengguna jasa melaksanakan transaksi impor dan/atau ekspor dengan jumlah yang melebihi batas maksimum nilai transaksi sesuai ketentuan, namun tidak menyediakan *underlying transaction*.

11. Pengguna jasa melakukan lebih dari satu kali transaksi impor dan/atau ekspor dengan jumlah yang melebihi batas maksimum nilai transaksi sesuai ketentuan, dengan *underlying transaction* berupa dokumen dengan format yang selalu sama, dan diduga palsu.

12. Pengguna jasa orang perseorangan melakukan transfer dana ke banyak rekening yang dimiliki oleh perusahaan di luar negeri dengan *underlying transaction* berupa *invoice* pembelian berbagai jenis barang.

13. Pengguna jasa merupakan perusahaan dengan profil perdagangan umum dan melakukan transfer dana ke beberapa pihak di luar negeri, dengan *underlying transaction* berupa *invoice* pembelian berbagai jenis barang.

14. Pengguna jasa dari beberapa perusahaan yang teridentifikasi memiliki *beneficial owner* 1 (satu) orang, dengan 1 (satu) alamat tempat usaha, dan dikuasakan kepada 1 (satu) orang yang sama, untuk melakukan transaksi keuangan dan/atau kuasa debet.

15. Pengguna jasa melakukan transaksi keuangan pada jaringan kantor bank yang berganti-ganti termasuk berada dalam satu lokasi atau berdekatan dengan kediaman atau apartemen tempat pengguna jasa berdomisili.

16. Pengguna jasa merupakan perusahaan yang terindikasi melakukan penutupan rekening, yang diikuti dengan pembukaan rekening baru, dengan dokumen perusahaan yang berbeda.

17. Perusahaan teridentifikasi sebagai perusahaan yang sama berdasarkan kesamaan nama pemilik dan/atau pengurus perusahaan.

18. Penempatan deposito yang tidak jelas sumber dananya.

19. Pembelian properti dengan menggunakan uang tunai.

20. Pembelian polis asuransi kerugian dengan harga yang lebih tinggi dibandingkan dengan harga properti.

21. Kepemilikan rekening uang asing dalam jumlah besar yang tidak berhubungan dengan pengguna jasa.

22. Memiliki beberapa kartu identitas atau dokumen perjalanan dengan nama yang berbeda-beda.

23. Memiliki beberapa kartu identitas dengan foto yang sama tetapi biodata yang berbeda.

24. Nasabah yang memaksa bertransaksi dengan petugas bank dan/atau petugas KUPVA BB/transfer dana yang sama setiap kali bertransaksi.

25. Kekayaan yang berlebihan atau tidak wajar.

26. Pelunasan utang dipercepat.

27. Cek atas nama perusahaan yang ditransfer ke dalam rekening pribadi.

28. Penempatan dana dalam jumlah besar yang tidak sebanding dengan pengiriman dana, misalnya penempatan deposito dengan nominal yang lebih besar dari nominal transfer dana yang digunakan untuk penempatan deposito tersebut.

29. Transfer dana dari rekening orang perseorangan yang kemudian rekening tersebut ditutup setelah transaksi transfer dana selesai dilakukan.

B. Transaksi yang Patut Diduga Dilakukan dengan Tujuan untuk Menghindari Pelaporan Transaksi yang Bersangkutan yang Wajib Dilakukan oleh PJK Sesuai dengan Ketentuan UU TPPU:

1. Transaksi yang dilakukan dengan menggunakan beberapa rekening atas nama individu yang berbeda beda untuk kepentingan satu orang tertentu (*smurfing*).

2. Transaksi dana masuk didominasi oleh transaksi setor tunai via mesin setor tunai dalam frekuensi yang tinggi dengan total dana yang besar.

C. Transaksi yang Dilakukan atau Batal Dilakukan dengan Menggunakan Harta Kekayaan yang Diduga Berasal dari Hasil Tindak Pidana:

1. PJK mengetahui bahwa pengguna jasa merupakan subyek dari penyelidikan/ penyidikan tindak pidana pencucian uang yang berasal dari tindak pidana narkotika, atau adanya keterkaitan antara orang yang diduga melakukan pencucian uang dengan pelaku tindak pidana narkotika.

2. PJK mendapatkan informasi dari sumber yang dapat dipercaya (PPATK, LPP, Aparat Penegak Hukum, media massa, atau sumber lainnya) bahwa pengguna jasa diduga terlibat dalam aktivitas ilegal dan/atau memiliki latar belakang terkait tindak pidana narkotika Pengguna jasa sering melakukan transaksi dengan para pihak yang sudah menjadi tersangka/terdakwa/terpidana tindak pidana pencucian uang dan/atau tindak pidana narkotika.

3. Keterangan transaksi memuat kode atau istilah tertentu.

4. Pengguna jasa sering melakukan transaksi dengan penyidik narkotika atau pegawai Lapas/Rutan (termasuk keluarga) tanpa *underlying transaction* yang jelas.

5. Pengguna jasa sering melakukan transaksi dengan pihak yang telah masuk dalam Daftar Pencarian Orang (DPO) terkait dugaan tindak pidana narkotika.

6. Rekening orang perseorangan menerima dana masuk dari banyak pengirim yang berbeda-beda.

7. Transaksi tarik tunai dengan frekuensi tinggi di wilayah lintas batas negara (*cross border*) yang rawan peredaran narkotika.

8. Pengguna jasa menerima dana hanya dari beberapa pihak saja dengan total nominal yang sangat besar, kemudian ditransfer ke banyak pihak dengan nominal yang kecil.

9. Terdapat transaksi yang masih aktif pada rekening dengan identitas yang sudah tidak berlaku lagi.

10. Pengguna jasa sering melakukan transaksi dengan pihak yang terkena sanksi dari OFAC (Office of Foreign Asset Control) Amerika Serikat.

11. Pengguna jasa melakukan transaksi dengan menggunakan internet banking yang berlokasi di Lembaga pemasyarakatan (lapas).

12. Transaksi pengiriman dana dengan menggunakan dokumen palsu.

D. Transaksi yang Diminta oleh PPATK untuk Dilaporkan oleh PJK karena Melibatkan Harta Kekayaan yang Diduga Berasal dari Hasil Tindak Pidana:

1. Transaksi Keuangan yang diminta oleh PPATK karena pengguna jasa telah ditetapkan sebagai tersangka/terdakwa dalam kasus TPPU dan/atau TP narkotika.

2. Transaksi keuangan oleh pengguna jasa yang diminta oleh PPATK karena keterkaitannya dengan transaksi lain terkait TPPU dan/atau TP narkotika yang sedang dalam proses analisis maupun pemeriksaan oleh PPATK.

3. Transaksi keuangan oleh pengguna jasa yang diminta oleh PPATK atas dasar penyelidikan atau penyidikan terkait TPPU dan/atau TP narkotika yang sedang dilakukan oleh Aparat Penegak Hukum.

2.4.5 Korupsi

Merujuk pada SRA TPPU Hasil Tindak Pidana Korupsi (2022), secara umum terdapat beberapa tipologi korupsi sebagai berikut:

a. Pemanfaatan korporasi (*legal person*).

b. Penggunaan *nominees* (nama pinjaman), *trusts*, anggota keluarga atau pihak ketiga.

c. Properti/*real estate* termasuk peran agen *property*.

d. *Mingling* (penyatuan uang haram dalam bisnis legal).

Secara khusus terdapat *Red Flag* yang perlu diwaspadai oleh penyelenggara sebagai berikut:

1. Menempatkan uang hasil TP ke dalam rekening perbankan melalui *nominee*.

2. Penukaran hasil tindak kejahatan ke dalam valuta asing (valas).

3. Keterlibatan BO perusahaan dalam kesepakatan pengadaan.

4. Penerimaan *fee* melalui rekening perusahaan cangkang yang didirikan di negara *tax heaven*.

5. Menggunakan metode *back to back loan*[3] dalam pembelian aset.

6. Menempatkan atau mentransferkan uang menggunakan rekening milik orang lain.

7. Pembelian aset dengan menggunakan nama orang lain.

8. Menukarkan uang hasil tindak pidana di penyelenggara KUPVA BB dalam jumlah yang signifikan.

9. Penukaran mata uang asing yang selalu di bawah atau mendekati Rp500.000.000 untuk menghindari pelaporan dan dilakukan pada hari yang sama atau berdekatan.

10. Pembayaran Kartu Kredit yang melebihi batas limit agar mendapatkan pengembalian kelebihan pembayaran untuk menyamarkan transaksi kartu kredit seolah-olah berasal dari transaksi yang sah.

11. Pembelian asset dengan menggunakan uang tunai dengan jumlah yang signifikan.

12. Pentransferan uang dalam jumlah yang signifikan yang tidak sesuai dengan profil.

13. Penyetoran uang tunai dalam jumlah yang signifikan yang berasal dari penukaran mata uang asing.

14. Pembelian aset dengan menggunakan nama orang lain.

[3]Pinjaman didukung dengan agunan berupa deposito/simpanan yang dimiliki debitur di bank terkait.

15. Rekening atas nama perusahaan dikuasakan kepada pihak lain diluar struktur kepengurusan perusahaan.

16. Pembelian asset berupa tanah dengan menggunakan nama kepemilikan orang lain atau pihak keuarga.

2.4.6 Kehutanan dan Lingkungan Hidup (*Green Financial Crime*/GFC)

A. Tipologi TPPU dan TPPT TPA Kehutanan

Merujuk pada SRA TPPU Hasil Tindak Pidana Kehutanan (2020), beberapa tipologi dari TPA Kehutanan sebagai berikut:

1. Terdapat transaksi yang dilakukan dengan para pihak terduga dan/atau terpidana melakukan aktivitas tindak pidana kehutanan.

2. Pengajuan fasilitas pembiayaan dengan menjaminkan lahan hutan lindung di wilayah yang tidak memiliki izin penggunaan kawasan; atau wilayah yang memiliki izin penggunaan kawasan, namun pelaku tidak memiliki izin yang sah (atau sudah tidak berlaku) untuk menggarap kawasan tersebut.

3. Adanya instruksi transaksi yang tidak wajar pada berita transaksi.

4. Transaksi tampak tidak sesuai atau tidak konsisten dengan aktivitas atau kegiatan bisnis pengguna jasa.

5. Penggunaan rekening pribadi atau perseorangan untuk menampung hasil kegiatan usaha.

6. Adanya transaksi dari rekening pengurus atau perusahaan di bidang kehutanan kepada pihak PEP (Pejabat Eksekutif, Legislatif dan Yudikatif).

7. Adanya setoran dan/atau penarikan uang tunai yang dipecah-pecah dengan nominal tertentu dan dilakukan berkali-kali dalam sehari (*structuring*).

8. Transaksi yang dilakukan secara tunai dalam jumlah besar diluar kebiasan pengguna jasa.

9. Identitas profil pekerjaan pengguna jasa saat pembukaan rekening tidak sesuai dengan jabatan dan pekerjaan saat ini.

10. Pola transaksi bersifat *pass-by* dengan transfer yang dilakukan secara mandiri oleh pengguna jasa.

11. Adanya pemanfaatan rekening lainnya sebagai rekening penampungan.

12. Adanya penggunaan rekening pribadi untuk melakukan aktivitas usaha yang mengatasnamakan beberapa perusahaan (*Beneficial Ownership*).

B. Tipologi TPPU dan TPPT TPA Lingkungan Hidup

Merujuk pada FATF Report – Money Laundering from Environmental Crime (2021), terdapat beberapa tipologi dari TPA Lingkungan Hidup sebagai berikut:

1. Penggunaan *front companies* untuk menggabungkan hasil legal dan illegal.

2. Penggunaan *shell company* untuk menyembunyikan *Beneficial Ownership* (BO).

3. *Trade based fraud* (proses menyamarkan hasil kejahatan dan pemindahan barang ke negara transit untuk menggabungan perdagangan barang legal dan barang ilegal (*co-mingling*), melalui penggunaan transaksi perdagangan untuk melegitimasi asal-usul uang/harta kekayaan yang berasal dari hasil tindak pidana).

4. *Trade based money laundering* (proses menyamarkan hasil kejahatan dan perubahan nilai melalui penggunaan transaksi perdagangan internasional untuk melegitimasi asal-usul uang/harta kekayaan yang berasal dari hasil tindak pidana).

5. Penggunaan PJK Regional dan Internasional.

Merujuk pada hasil laporan TKM dan hasil putusan pengadilan TP Lingkungan Hidup, tipologi sebagai berikut:

1. **Transaksi yang Menyimpang Profil, Karakteristik atau Kebiasaan Pola Transaksi Pengguna Jasa yang Bersangkutan:**

   a) Transaksi usaha di bidang industri pencelupan dan penyempurnaan kain pengolahan tekstil dengan melakukan pemecahan transaksi menggunakan rekening karyawan untuk kepentingan perusahaan.

   b) Transaksi yang tidak sesuai atau tidak konsisten dengan aktivitas atau kegiatan bisnis pengguna jasa

2. **Transaksi yang Patut Diduga Dilakukan dengan Tujuan untuk Menghindari Pelaporan Transaksi yang Bersangkutan yang Wajib Dilakukan oleh PJK Sesuai dengan Ketentuan UU TPPU:**

   Pemberian kuasa pengguna rekening individu kepada pihak yang terdaftar dalam struktur perusahaan dan pemberian kuasa substitusi pada rekening individu.

3. **Transaksi yang Dilakukan atau Batal Dilakukannya dengan Menggunakan Harta Kekayaan yang Diduga Berasal dari Tindak Pidana:**

   PJK mendapatkan informasi dari sumber yang dapat dipercaya (PPATK, Pengawas, Apgakum, sumber lain) bahwa pengguna jasa diduga terlibat dalam aktivitas illegal dan/atau memiliki latar belakang tindak kriminal.

BAGIAN 3

HASIL RISET

3.1 Gambaran Putusan TPPU, TPPT, dan PPSPM

3.1.1 Profil Penyelenggara Media TPPU, TPPT, dan PPSPM

A. Profil Penyelenggara Media TPPU

Berdasarkan data putusan pengadilan TPPU tahun 2015-2020, profil penyelenggara yang dominan dijadikan media pencucian uang adalah **"KUPVA Bukan Bank"**. Dari total 24 (dua puluh empat) kasus TPPU, terdapat 22 (dua puluh dua) kasus TPPU yang terjadi di Penyelenggara KUPVA Bukan Bank. Sementara itu, 2 (dua) kasus lainnya terjadi di PTD Bukan Bank. Adapun tren putusan TPPU berdasarkan jenis penyelenggara yang menjadi media pencucian uang sebagaimana pada tabel berikut:

Tabel 3.1. Tren Putusan TPPU Berdasarkan Jenis Penyelenggara

Profil Penyelenggara	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
KUPVA Bukan Bank		2	4	4	8	4
PTD Bukan Bank					1	1

Sumber: PPATK, Diolah

B. Profil Penyelenggara Media TPPT

Berdasarkan data putusan pengadilan TPPT tahun 2015-2020, profil penyelenggara yang dominan dijadikan media pendanaan terorisme adalah **"PTD Bukan Bank"**. Terdapat 4 (empat) dari 5 (lima) kasus TPPT yang terjadi di PTD Bukan Bank. Sementara itu, 3 (tiga) kasus terjadi di Penyelenggara KUPVA Bukan Bank. Adapun tren putusan TPPT berdasarkan jenis penyelenggara yang menjadi media pendanaan terorisme sebagaimana pada tabel berikut:

Tabel 3.2. Tren Putusan TPPT Berdasarkan Jenis Penyelenggara

Profil Penyelenggara	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
KUPVA Bukan Bank			1	1		1
PTD Bukan Bank	1	1	1	1		

Sumber: PPATK, Diolah

Sementara itu, berdasarkan data putusan pengadilan tahun 2015-2020 belum ditemukan adanya kasus terkait PPSPM.

3.1.2 Profil Pelaku Perorangan TPPU, TPPT, dan PPSPM

A. Profil Pelaku Perorangan TPPU

Berdasarkan data putusan pengadilan TPPU tahun 2015-2020, profil pekerjaan pelaku pencucian uang yang dominan adalah **"Pengusaha/Wiraswasta"**. Dari total 24 (dua puluh empat) kasus TPPU, terdapat 16 (enam belas) orang pelaku perorangan yang berprofesi sebagai Wiraswasta. Sementara itu, profil pekerjaan lainnya adalah Pegawai Swasta sebanyak 7 (tujuh) orang; PNS, Pejabat Pemerintahan, dan lainnya dengan masing-masing sebanyak 2 (dua) orang; serta Ibu Rumah Tangga, Pegawai *Money Changer*, dan

Pengajar dengan masing-masing sebanyak 1 (satu) orang. Adapun tren putusan TPPU berdasarkan profil pelaku perorangan sebagaimana pada tabel berikut:

Tabel 3.3. Tren Putusan TPPU Berdasarkan Profil Pelaku Perorangan

Profil Pekerjaan	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
Pengusaha/ Wiraswasta		2	2	5	4	3
Pegawai Swasta					6	1
PNS (Termasuk Pensiunan)			2			
Ibu Rumah Tangga					1	
Pejabat LembagaLegislatif dan Pemerintah			1			1
Pegawai *Money Changer*					1	
Pengajar dan Dosen					1	
Lainya					1	1

Sumber: PPATK, Diolah

B. Profil Pelaku Perorangan TPPT

Berdasarkan data putusan pengadilan TPPT tahun 2015-2020, dari total 5 (lima) kasus TPPT, terdapat 1 (satu) orang pelaku yang berprofesi sebagai **"Pengusaha/Wiraswasta"**. Selanjutnya, terdapat 1 (satu) orang pelaku yang tidak bekerja. Selain itu, terdapat 3 (tiga) orang pelaku yang profil pekerjaannya tidak dapat diidentifikasi. Adapun tren putusan TPPT berdasarkan profil pelaku perorangan antara lain:

Tabel 3.4. Tren Putusan TPPT Berdasarkan Profil Pelaku Perorangan

Profil Pekerjaan	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
Pengusaha/ Wiraswasta			1			
Tidak Bekerja				1		
Tidak Teridentifikasi	1	1				1

Sumber: PPATK, Diolah

Sementara itu, berdasarkan data putusan pengadilan tahun 2015-2020 belum ditemukan adanya kasus terkait PPSPM.

3.1.3. Profil Pelaku Badan Usaha TPPU, TPPT, dan PPSPM

A. Profil Pelaku Badan Usaha TPPU

Berdasarkan data putusan pengadilan TPPU tahun 2015-2020, profil badan usaha yang terlibat dalam pencucian uang didominasi oleh **"Perusahaan Non UMKM berbentuk Perseroan Terbatas (PT)"**. Terdapat 11 (sebelas) dari 24 (dua puluh empat) kasus melibatkan PT. Sementara itu, profil badan usaha lainnya adalah Perusahaan Non UMKM berbentuk Persekutuan Komanditer (CV), yang terlibat pada 3 (tiga) kasus. Selain itu, terdapat 11 (sebelas) kasus yang tidak dapat diidentifikasi profil badan usahanya atau tidak melibatkan badan usaha. Adapun tren putusan TPPU berdasarkan profil badan usaha sebagaimana pada tabel berikut:

Tabel 3.5. Tren Putusan TPPU Berdasarkan Profil Pelaku Badan Usaha

Profil Badan Usaha	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
Perusahaan Non UMKM Berbentuk Perseroan terbatas (PT)		1		3	5	2
Perusahaan Non UMKM Berbentuk Persekutuan Komanditer (CV)					2	1
Tidak Teridentifikasi		1	4	1	2	3

Sumber: PPATK, Diolah

Sementara itu, berdasarkan data putusan pengadilan TPPT tahun 2015-2020, dari total 5 (lima) kasus TPPT, tidak dapat diidentifikasi apakah terdapat profil badan usaha yang terlibat dalam praktik pendanaan terorisme. Selanjutnya, berdasarkan data putusan pengadilan tahun 2015-2020 belum ditemukan adanya kasus terkait PPSPM.

3.1.4 Wilayah TPPU, TPPT, dan PPSPM

A. Wilayah TPPU

Berdasarkan data putusan pengadilan TPPU tahun 2015-2020, terdapat 4 (empat) provinsi sebaran wilayah putusan perkara pencucian uang selama tahun 2015-2020. Putusan pengadilan tersebut sebagian besar berada di **"DKI Jakarta"**. Dari total 24 (dua puluh empat), terdapat 20 (dua puluh) kasus terjadi di DKI Jakarta. Sementara itu, provinsi lainnya adalah Kalimantan Barat sebanyak 2 (dua) kasus, serta Banten dan Lampung dengan masing-masing sebanyak 1 (satu) kasus. Adapun tren putusan TPPU berdasarkan wilayah antara lain:

Tabel 3.6. Tren Putusan TPPU Berdasarkan Wilayah Geografis

Wilayah	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
DKI Jakarta		2	4	4	7	3
Kalimantan Barat					1	1
Banten					1	
Lampung						1

Sumber: PPATK, Diolah

B. Wilayah TPPT

Berdasarkan data putusan pengadilan TPPT tahun 2015-2020, terdapat 5 (lima) kasus TPPT, dimana 3 (tiga) kasus berada di **"DKI Jakarta"**. Namun demikian, untuk 2 (dua) kasus lainnya tidak dapat diidentifikasi wilayah tempat terjadinya tindak pidana. Adapun tren putusan TPPT berdasarkan wilayah sebagai berikut:

Tabel 3.7. Tren Putusan TPPT Berdasarkan Wilayah Geografis

Wilayah	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
DKI Jakarta			1	1		1
Tidak Teridentifikasi	1	1				

Sumber: PPATK, Diolah

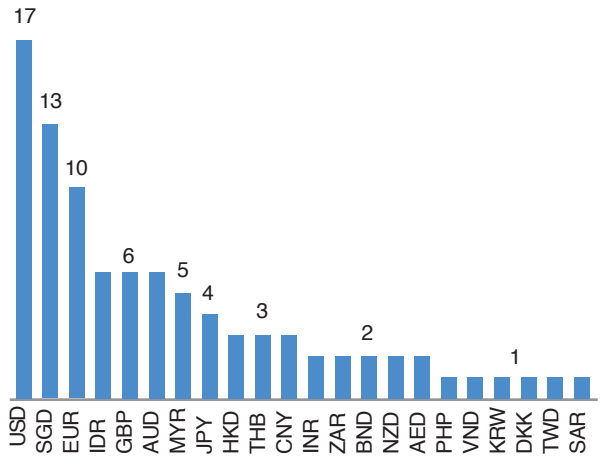
Sementara itu, berdasarkan data putusan pengadilan tahun 2015-2020 belum ditemukan adanya kasus terkait PPSPM.

3.1.5 Produk dan Layanan TPPU, TPPT, dan PPSPM

A. Produk dan Layanan TPPU

Berdasarkan data putusan pengadilan TPPU tahun 2015-2020, jika ditinjau berdasarkan produk Uang Kertas Asing (UKA) yang ditransaksikan pada Penyelenggara KUPVA Bukan Bank, UKA yang dominan digunakan dalam pencucian uang adalah **"USD"**. Dari total 22 (dua puluh dua) kasus, terdapat 17 (tujuh belas) kasus yang melibatkan penggunaan USD, diikuti SGD sebanyak 13 (tiga belas) kasus, dan EUR sebanyak 10 (sepuluh) kasus. Sementara itu, jenis UKA lainnya yang digunakan dalam pencucian uang dapat dilihat pada grafik berikut:

Grafik 3.1. Jumlah Putusan Pada Penyelenggara KUPVA Bukan Bank Berdasarkan Produk UKA



Sumber: PPATK, Diolah

Lebih lanjut, mekanisme jual beli UKA yang dominan digunakan dalam pencucian uang melalui Penyelenggara KUPVA Bukan Bank adalah **"Transfer Bank"**. Dari total 22 (dua puluh dua) kasus, terdapat 15 (lima belas) kasus yang melibatkan penggunaan layanan Transfer Rupiah melalui Bank. Diikuti dengan 7 (tujuh) kasus yang menggunakan mekanisme Tunai baik penyerahan UKA maupun Rupiah secara tunai. Namun demikian, terdapat 2 (dua) kasus yang tidak dapat diidentifikasi mekanisme yang digunakan pada transaksi jual beli UKA yang dilakukan.

Sementara itu, produk dan layanan yang digunakan dalam pencucian uang melalui PTD Bukan Bank adalah ***"Cast to Account (Outgoing)"*** dan ***"Account to Account (Incoming)"*** dengan total sebanyak 2 (dua) kasus. Adapun tren putusan TPPU berdasarkan produk dan layanan antara lain:

Tabel 3.8. Tren Putusan TPPU Berdasarkan Produk dan Layanan

Produk dan Layanan	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
KUPVA Bukan Bank						
Transfer Bank		2	2	4	7	
Tunai (UKA dan Rupiah)		1		3		3
Jual Beli UKA					1	1
PTD Bukan Bank						
Account to Account (*Incoming*)					1	
Cash to Account (*Outgoing*)						1

Sumber: PPATK, Diolah

B. Produk dan Layanan TPPT

Berdasarkan data putusan pengadilan TPPT tahun 2015-2020, jika ditinjau berdasarkan produk UKA yang ditransaksikan pada Penyelenggara KUPVA Bukan Bank, UKA yang dominan digunakan dalam pendanaan terorisme adalah **"USD".** Dari 3 (tiga) kasus yang menggunakan Penyelenggara KUPVA Bukan Bank sebagai media pendanaan terorisme, 2 (dua) kasus menggunakan USD. Terdapat 1 (satu) kasus yang menggunakan beberapa jenis produk UKA selain USD, antara lain MYR, KHR, PHP, dan VND. Sementara itu, 1 (satu) kasus lainnya tidak dapat diidentifikasi produk UKA yang digunakan.

Lebih lanjut, berdasarkan analisis putusan pengadilan TPPT pada KUPVA Bukan Bank, terdapat 2 (dua) kasus yang tidak dapat diidentifikasi mekanisme jual beli UKA yang digunakan oleh pelaku tindak pidana. Mekanisme jual beli UKA yang dimaksud dalam hal ini adalah mekanisme Transfer Rupiah maupun penyerahan secara Tunai untuk UKA atau Rupiah. Sementara itu, terdapat 1 (satu) kasus yang tidak dapat diidentifikasi kegiatan usaha yang dijadikan media pendanaan terorisme. Kegiatan usaha yang dimaksud dalam hal ini adalah jual beli UKA, pembelian cek pelawat, ataupun pembawaan UKA lintas batas negara.

Pada kasus TPPT yang melibatkan PTD Bukan Bank, produk/layanan yang dominan digunakan adalah **"*Cash to Account (Outgoing)*"**. Dari 4 (empat) kasus yang menggunakan PTD Bukan Bank sebagai media pendanaan terorisme, terdapat 2 (dua) kasus yang memanfaatkan produk/layanan *Cash to Account (Outgoing)*. Selain itu, terdapat 1 (satu) kasus yang melibatkan penggunaan layanan *Account to Account (Outgoing)* dan 1 (satu) kasus yang tidak teridentifikasi produk/layanan yang digunakan. Adapun tren putusan TPPT berdasarkan produk dan layanan sebagai berikut:

Tabel 3.9. Tren Putusan TPPT Berdasarkan Produk dan Layanan

Produk dan Layanan	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
Kantor KUPVA						
Jual Beli UKA			1	1		
Tidak Teridentifikasi						1
Kantor PTD						
Cash to Account (*Outgoing*)			1	1		
Account to Account (*Outgoing*)		1				
Tidak Teridentifikasi	1					

Sumber: PPATK, Diolah

Sementara itu, berdasarkan data putusan pengadilan tahun 2015-2020 belum ditemukan adanya kasus terkait PPSPM.

3.1.6 *Delivery Channel* TPPU, TPPT, dan PPSPM

A. *Delivery Channel* TPPU

Berdasarkan data putusan pengadilan TPPU tahun 2015-2020, *delivery channel* yang dominan digunakan dalam pencucian uang adalah **"Kantor KUPVA"**. Dari total 24 (dua puluh empat) kasus, terdapat 22 (dua puluh dua) kasus yang melibatkan Kantor KUPVA. Dari 22 (dua puluh dua) kasus yang melibatkan Kantor KUPVA, terdapat 15 (lima belas) kasus yang menggunakan Kantor KUPVA hanya sebagai media pencucian uang. Namun demikian, sisanya yakni 7 (tujuh) kasus menggunakan Kantor KUPVA sebagai agen/pelaku pencucian uang. *Delivery channel* lainnya adalah Kantor PTD, yaitu sebanyak 2 (dua) kasus yang menggunakan Kantor PTD sebagai media pencucian uang. Adapun tren putusan TPPU berdasarkan *delivery channel* sebagai berikut:

Tabel 3.10. Tren Putusan TPPU Berdasarkan *Delivery Channel*

Delivery Channel	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
Kantor KUPVA		2	4	4	8	4
Kantor PTD					1	1

Sumber: PPATK, Diolah

B. *Delivery Channel* TPPT

Berdasarkan data putusan pengadilan TPPT tahun 2015-2020, *delivery channel* yang dominan digunakan dalam pendanaan terorisme adalah **"Kantor PTD"**. Dari total 5 (lima) kasus TPPT yang terjadi, 4 (empat) kasus melibatkan penggunaan Kantor PTD. *Delivery channel* lainnya adalah Kantor KUPVA, dimana terdapat 3 (tiga) kasus yang melibatkan penggunaan Kantor KUPVA dalam pendanaan terorisme. Adapun tren putusan TPPT berdasarkan *delivery channel* sebagai berikut:

Tabel 3.11. Tren Putusan TPPT Berdasarkan *Delivery Channel*

Delivery Channel	Jumlah Putusan					
	2015	2016	2017	2018	2019	2020
Kantor KUPVA			1	1		1
Kantor PTD	1	1	1	1		

Sumber: PPATK, Diolah

Sementara itu, berdasarkan data putusan pengadilan tahun 2015-2020 belum ditemukan adanya kasus terkait PPSPM.

3.2 Tipologi TPPU, TPPT, dan PPSPM

3.2.1 Tipologi TPPU dan TPPT pada KUPVA Bukan Bank

A. Tipologi TPPU pada KUPVA Bukan Bank

Beberapa tipologi TPPU yang menggunakan penyelenggara KUPVA Bukan Bank berdasarkan hasil analisis putusan pengadilan tahun 2015-2020 serta hasil analisis studi literatur, antara lain:

1. Transaksi pembelian UKA dilakukan oleh pihak lain yang bukan sebagai penerima manfaat *(Beneficial Owner)*;
2. Penyerahan Rupiah dilakukan secara transfer, namun pengambilan UKA secara tunai dilakukan oleh orang lain;
3. Penyerahan UKA dilakukan secara tunai, namun penyerahan Rupiah dilakukan secara transfer ke rekening orang lain atau transfer ke beberapa rekening.
4. Penyerahan Rupiah dilakukan secara transfer ke beberapa rekening *(smurfing)* yang dimiliki 1 (satu) individu atau entitas *beneficial owner*. Rekening tujuan biasanya menggunakan *nominees* (nama pinjaman), *trusts*, anggota keluarga, atau pihak ketiga.
5. Transaksi yang dilakukan tidak sesuai dengan profil pengguna jasa;
6. Pembelian UKA dengan uang tunai dalam jumlah besar dan pengguna jasa menolak atau mengalami kesulitan untuk menginformasikan sumber dana atau uang tunai;
7. Transaksi penukaran UKA dalam jumlah yang signifikan dan jenis mata uang yang berbeda-beda dalam 1 (satu) kali transaksi;
8. Transaksi penukaran UKA dalam jumlah signifikan oleh *Politically Exposed Persons* (PEPs);
9. Transaksi dengan jumlah signifikan tanpa disertai *underlying transaction* yang jelas;
10. Penggunaan rekening individu/pribadi dalam operasional KUPVA Bukan Bank sebagai media/penampungan hasil kejahatan;
11. Penggunaan Penyelenggara KUPVA Bukan Bank tidak berizin;
12. Penggunaan identitas palsu saat melakukan penukaran valuta asing;
13. Transaksi tidak dibukukan ke dalam sistem KUPVA Bukan Bank dan tidak diberikan nota atas transaksi yang dilakukan;
14. Transaksi dalam jumlah relatif kecil, namun dilakukan dalam beberapa tahap dengan frekuensi yang tinggi dalam periode waktu tertentu (*structuring*). Transaksi juga seringkali dilakukan pada lebih dari satu KUPVA Bukan Bank dalam waktu dekat;
15. Transaksi *U-turn* menggunakan skema *telegraphic transfer* (T/T) dimana KUPVA Bukan Bank yang memiliki izin pembawaan UKA melakukan pembawaan UKA dari negara lain, kemudian dana ditransfer ke rekening lain dalam negeri, dan pada akhirnya dilakukan transfer kembali ke negara sumber dana;

16. *Trade Based Money Laundering, Transfer Pricing*, dan penggunaan Perusahaan Cangkang untuk menghasilkan *invoice* fiktif yang digunakan sebagai *underlying transaction* penukaran UKA pada KUPVA Bukan Bank. Perusahaan Cangkang juga digunakan untuk menyimpan aset *beneficial owner* yang diperoleh dari tindak kejahatan. Selain itu, rekening perusahaan juga digunakan untuk menerima dana hasil kejahatan.

17. Penukaran mata uang denominasi kecil ke denominasi besar dalam jumlah yang cukup banyak;

18. Penukaran dalam jumlah besar terhadap UKA yang jarang digunakan;

19. Penggabungan dana hasil kejahatan dengan dana hasil kegiatan usaha yang sah *(mingling)*.

Lebih lanjut, berdasarkan hasil Survei Tipologi TPPU/TPPT/PPSPM yang dilakukan terhadap 171 (seratus tujuh puluh satu) sampel KUPVA Bukan Bank yang berada di bawah pengaturan dan pengawasan Bank Indonesia, diperoleh tingkat risiko tipologi TPPU pada KUPVA Bukan Bank berdasarkan persepsi penyelenggara sebagai berikut:

Tabel 3.12. Tingkat Risiko Tipologi TPPU pada KUPVA Bukan Bank

Tipologi TPPU	Tingkat Risiko	Kategori Risiko
Penggunaan Identitas Palsu	5.65	Menengah
Mingling	5.63	Menengah
Trade Based Money Laundering dan *Transfer Pricing*	5.46	Menengah
Bank Ilegal/Pengiriman Dana Alternatif/Hawala	5.44	Menengah
Penyelundupan Manusia	5.40	Menengah
Pemanfaatan *Nominees, Trust,* Anggota Keluarga atau Pihak Ketiga	5.39	Menengah
Aktivitas Perjudian *Online*	5.39	Menengah
Pertukaran Komoditas	5.39	Menengah
Pemanfaatan Perusahaan Cangkang (*Shell Companies*) terhadap Uang Hasil Tindak Pidana Perpajakan	5.33	Menengah
Pemanfaatan Korporasi	5.26	Menengah
Transfer *Cross Border*	5.26	Menengah
Smurfing	5.25	Menengah
Pemanfaatan *Offshore Banks*, Perusahaan Bisnis Internasional dan *Trust* Lepas Pantai	5.25	Menengah
Pemanfaatan Internet Enkripsi, Akses terhadap Identitas, Perbankan Internasional	5.25	Menengah
Structuring	5.21	Menengah
Investasi di Pasar Modal, Penggunaan Perantara	5.18	Menengah
Pemanfaatan Kartu Kredit, Cek, Surat Perjanjian Hutang	5.14	Menengah
Pemanfaatan Jasa Profesi	5.12	Menengah
Perdagangan Perhiasan dan Logam Mulia	5.12	Menengah
Properti/*Real Estate*, termasuk peran agen Properti	5.07	Menengah
Pembelian Aset Berharga	5.05	Menengah
Pemanfaatan Mata Uang Virtual	5.04	Menengah
Pemanfaatan Inovasi Sistem Pembayaran	4.98	Rendah
Pemanfaatan Sektor Non Keuangan	4.96	Rendah

Berdasarkan hasil survei, tipologi pencucian uang pada KUPVA Bukan Bank yang memiliki risiko tertinggi adalah penggunaan identitas palsu, *mingling*, serta *trade-based money laundering* dan *transfer pricing*. Penggunaan identitas palsu menjadi salah satu tipologi yang berisiko tinggi karena terdapat kemudahan dalam pembuatan dokumen identitas palsu, serta kerentanan pada proses identifikasi dan verifikasi pengguna jasa. Pengguna jasa KUPVA Bukan Bank yang mayoritas merupakan *walk-in customer* memberikan kerentanan pada proses CDD karena dilakukan dalam waktu yang relatif singkat. Selain itu, pada aktualnya belum seluruh KUPVA Bukan Bank terkoneksi dengan data Kependudukan dan Catatan Sipil (Dukcapil), menyebabkan kurang optimalnya proses verifikasi identitas pengguna jasa.

Mingling[4] menjadi salah satu tipologi TPPU yang berisiko terjadi pada KUPVA Bukan Bank. Pada tipologi *mingling*, KUPVA Bukan Bank tidak hanya sebagai media pencucian uang, namun sebagai agen/pelaku pencucian uang. Tingginya potensi risiko tipologi *mingling* dilakukan melalui KUPVA Bukan Bank, sejalan dengan analisis hasil putusan pengadilan dimana terdapat motif pegawai *money changer* memanfaatkan KUPVA Bukan Bank sebagai media untuk menerima dan mentransfer dana. Selanjutnya, dana hasil pencucian uang juga dicampur dengan uang dari kegiatan usaha jual beli valas *(mingling)* untuk menyamarkan asal usul dana tersebut.

Tipologi TPPU *Trade-Based Money Laundering* dan *Transfer Pricing* juga rentan terjadi pada KUPVA Bukan Bank. *Trade Based Money Laundering, Transfer Pricing*, dan penggunaan Perusahaan Cangkang *(shell company)* sering disalahgunakan untuk menghasilkan *invoice* fiktif yang digunakan sebagai *underlying transaction* penukaran UKA pada KUPVA Bukan Bank.

[4]*Mingling*: Modus/tipologi TPPU dengan mencampurkan harta kekayaan hasil tindak pidana dengan usaha atau kegiatan yang sah

B. Tipologi TPPT pada KUPVA Bukan Bank

Beberapa tipologi TPPT yang menggunakan penyelenggara KUPVA Bukan Bank yaitu:

1. Transaksi pembelian UKA dilakukan oleh pihak lain yang bukan sebagai penerima manfaat (*Beneficial Owner*);
2. Transaksi yang dilakukan tidak sesuai dengan profil pengguna jasa;
3. *Structuring* yakni melakukan transaksi dalam jumlah relatif kecil, namun dilakukan dalam beberapa tahap dengan frekuensi yang tinggi;
4. Transaksi menggunakan dokumen identitas palsu.

Lebih lanjut, berdasarkan hasil Survei Tipologi TPPU/TPPT/PPSPM yang dilakukan terhadap 171 (seratus tujuh puluh satu) sampel KUPVA Bukan Bank yang berada di bawah pengaturan dan pengawasan Bank Indonesia, diperoleh tingkat risiko tipologi TPPT pada KUPVA Bukan Bank berdasarkan persepsi penyelenggara sebagai berikut:

Tabel 3.13. Tingkat Risiko Tipologi TPPT pada KUPVA Bukan Bank

Tipologi TPPT	Tingkat Risiko	Kategori Risiko
Penggunaan Dana: Operasi Terorisme Domestik - Pembelian Senjata dan Bahan Peledak	5.28	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Dokumen Identitas Palsu	5.28	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Perjalanan dari dan ke lokasi aksi terorisme	5.26	Menengah
Pengumpulan Dana - Ilegal: Hasil Kejahatan Kriminal Lainnya	5.25	Menengah
Penggunaan Dana: Operasi Terorisme Luar Negeri - Perjalanan Pejuang Teroris Asing	5.23	Menengah

Tipologi TPPT	Tingkat Risiko	Kategori Risiko
Penggunaan Dana: Gaji dan Kompensasi Anggota Kelompok Terorisme - Gaji Pimpinan dan Anggota Kelompok	5.21	Menengah
Pengumpulan Dana - Ilegal: Eksploitasi Sumber Daya Alam secara Ilegal	5.19	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Pembelian dan Perawatan Kendaraan atau Mesin	5.19	Menengah
Pengumpulan Dana - Ilegal: Pemerasan	5.18	Menengah
Penggunaan Dana: Pelatihan - Penggunaan Senjata dan Bahan Peledak	5.16	Menengah
Penggunaan Dana: Pelatihan - Pembuatan Senjata dan Bahan Peledak	5.16	Menengah
Pengumpulan Dana - Ilegal: Penculikan dengan Tebusan	5.14	Menengah
Pengumpulan Dana - Legal: Penyimpangan Pengumpulan Donasi Melalui Ormas	5.12	Menengah
Pemindahan Dana: Melalui Pembawaan Uang Tunai Lintas Batas	5.12	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Biaya Hidup Dasar (Pangan, Papan, Biaya Medis)	5.12	Menengah
Penggunaan Dana: Gaji dan Kompensasi Anggota Kelompok Terorisme - Santunan kepada Keluarga bagi Anggota yang Masuk Penjara atau Meninggal	5.12	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Biaya Kurir (Pengiriman Pesan, Uang)	5.09	Menengah
Penggunaan Dana: Pelatihan - Ideologi	5.09	Menengah

Tipologi TPPT	Tingkat Risiko	Kategori Risiko
Pengumpulan Dana - Legal: Sponsor Pribadi (*Terrorist Financier/ Fundraiser*)	5.07	Menengah
Penggunaan Dana: Pelatihan - Komunikasi Rahasia/Sandi	5.02	Menengah
Pemindahan Dana: Menggunakan Metode Pembayaran Baru	5.00	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan dan Pemeliharaan akun di Media Sosial	4.96	Rendah
Pemindahan Dana: Melalui Penyedia Jasa Keuangan	4.95	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan dan Pemeliharaan Situs Web	4.95	Rendah
Pemindahan Dana: Melalui Penyedia Barang dan Jasa	4.88	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan Majalah atau Koran	4.88	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Media Promosi Lainnya (televisi, radio)	4.88	Rendah
Penggunaan Dana: Pelatihan - Pelatihan *Virtual/Online*	4.88	Rendah
Pengumpulan Dana - Legal: Pendanaan *Crowdfunding*	4.81	Rendah
Pemindahan Dana: Melalui Profesi	4.81	Rendah
Pengumpulan Dana - Legal: Pendanaan Mandiri (Selain dari Usaha Bisnis)	4.58	Rendah
Pengumpulan Dana - Legal: Usaha Bisnis yang Sah	4.35	Rendah

Berdasarkan hasil survei, tipologi pendanaan terorisme pada KUPVA Bukan Bank yang memiliki risiko tertinggi adalah Penggunaan Dana: Operasi Terorisme Domestik - Pembelian Senjata dan Bahan Peledak, Penggunaan Dana: Operasi Terorisme Domestik - Dokumen Identitas Palsu, serta Penggunaan Dana: Operasi Terorisme Domestik - Perjalanan dari dan ke lokasi aksi terorisme.

KUPVA Bukan Bank pada dasarnya rentan digunakan sebagai media pendanaan terorisme khususnya pada tahap penggunaan dana *(using)*. Berdasarkan analisis hasil putusan pengadilan, pelaku memanfaatkan KUPVA Bukan Bank untuk melakukan penukaran rupiah/valas. Dana selanjutnya digunakan untuk biaya perjalanan ke lokasi aksi terorisme serta pembelian senjata api.

3.2.2 Tipologi TPPU dan TPPT pada PTD Selain Bank

A. Tipologi TPPU pada PTD Selain Bank

Beberapa tipologi TPPU yang menggunakan PTD Selain Bank yaitu:

1. PTD Bukan Bank berizin bekerja sama dengan PTD Bukan Bank tidak berizin untuk mengirimkan atau menerima dana;

2. Transaksi dalam jumlah relatif kecil, namun dilakukan secara bertahap dengan frekuensi yang tinggi (*structuring*);

3. Transaksi pengiriman dana melalui beberapa PTD Bukan Bank dengan tujuan penerima yang sama;

4. Transaksi PTD Bukan Bank tampak tidak sesuai atau tidak konsisten dengan aktivitas usahanya. Misalnya PTD Bukan Bank didirikan untuk memberikan layanan pengiriman uang dari TKI yang bekerja di luar negeri, namun tidak terdapat transaksi valuta asing yang signifikan dari luar negeri. Transaksi masuk pada rekening usaha tersebut mayoritas bersumber dari transaksi dalam negeri;

5. Menerima transaksi *incoming* yang diikuti dengan transaksi *outgoing* dalam waktu dekat;

6. Menggunakan dokumen identitas palsu atau yang memuat data fiktif atau tidak valid;

7. Melakukan pencairan dana yang diterima dari beberapa rekening (*smurfing*).

Lebih lanjut, berdasarkan hasil Survei Tipologi TPPU/TPPT/PPSPM yang dilakukan terhadap 48 (empat puluh delapan) sampel PTD Selain Bank yang berada di bawah pengaturan dan pengawasan Bank Indonesia, diperoleh tingkat risiko tipologi TPPU pada PTD Selain Bank berdasarkan persepsi penyelenggara sebagai berikut:

Tabel 3.14. Tingkat Risiko Tipologi TPPU pada PTD Bukan Bank

Tipologi TPPU	Tingkat Risiko	Kategori Risiko
Smurfing	5,88	Menengah
Aktivitas Perjudian Online	5,88	Menengah
Structuring	5,81	Menengah
Penyelundupan Manusia	5,81	Menengah
Pertukaran Komoditas	5,81	Menengah
Pemanfaatan Perusahaan Cangkang (*Shell Companies*) terhadap Uang Hasil Tindak Pidana Perpajakan	5,69	Menengah
Mingling	5,69	Menengah
Penggunaan Identitas Palsu	5,63	Menengah
Bank Ilegal/Pengiriman Dana Alternatif/Hawala	5,63	Menengah

Tipologi TPPU	Tingkat Risiko	Kategori Risiko
Pemanfaatan *Nominees, Trust*, Anggota Keluarga atau Pihak Ketiga	5,63	Menengah
Trade Based Money Laundering dan *Transfer Pricing*	5,56	Menengah
Transfer *Cross Border*	5,56	Menengah
Pemanfaatan Korporasi	5,50	Menengah
Pemanfaatan Jasa Profesi	5,50	Menengah
Properti/*Real Estate*, termasuk peran agen Properti	5,50	Menengah
Pemanfaatan Mata Uang Virtual	5,44	Menengah
Pemanfaatan Internet Enkripsi, Akses terhadap Identitas, Perbankan Internasional	5,44	Menengah
Pembelian Aset Berharga	5,44	Menengah
Pemanfaatan *Offshore Banks*, Perusahaan Bisnis Internasional dan *Trust* Lepas Pantai	5,38	Menengah
Perdagangan Perhiasan dan Logam Mulia	5,38	Menengah
Penukaran Uang Asing	5,31	Menengah
Pemanfaatan Inovasi Sistem Pembayaran	5,19	Menengah
Pemanfaatan Sektor Non Keuangan	5,19	Menengah
Pemanfaatan Kartu Kredit, Cek, Surat Perjanjian Hutang	5,19	Menengah
Investasi di Pasar Modal, Penggunaan Perantara	5,13	Menengah

Berdasarkan hasil survei, tipologi pencucian uang pada PTD Selain Bank yang memiliki risiko tertinggi adalah *smurfing*, aktivitas perjudian *online*, dan *structuring*. *Smurfing* dan *structuring* merupakan salah satu tipologi yang berisiko terjadi pada PTD Selain Bank karena terdapat potensi kerentanan dari penyelenggara dalam melakukan pemantauan profil maupun transaksi pengguna jasa. Lebih lanjut, tipologi *smurfing* yang melibatkan aliran dana dari berbagai pihak menyebabkan penyelenggara serta otoritas terkait mengalami kesulitan dalam mendeteksi transaksi keuangan yang dianggap mencurigakan. Publikasi *Money Laundering through Money Remittance and Currency Exchange Providers* FATF 2010 turut mengkonfirmasi bahwa *structuring* dan *smurfing* yang bertujuan untuk memecah transaksi dan melibatkan pengiriman dana ke rekening beberapa pihak, merupakan tipologi pencucian uang yang mayoritas ditemukan pada PTD Selain Bank.

Sementara itu, aktivitas perjudian *online* juga menjadi salah satu tipologi TPPU yang berisiko terjadi pada PTD Selain Bank. Kerentanan pada pengawasan dan pendeteksian aktivitas perjudian *online* ilegal serta aliran dananya memberikan potensi risiko TPPU, khususnya apabila dilakukan melalui PTD Selain Bank.

B. Tipologi TPPT pada PTD Selain Bank

Beberapa modus TPPT yang menggunakan PTD Selain Bank yaitu:

1. PTD Selain Bank yang berizin bekerja sama dengan PTD Selain Bank yang tidak berizin untuk mengirimkan dana;
2. Transaksi dalam jumlah relatif kecil, namun dilakukan secara bertahap dengan frekuensi yang tinggi (*structuring*);
3. Transaksi *incoming* dari beberapa negara berisiko tinggi dan frekuensi transaksi yang cukup tinggi;
4. Transaksi pengiriman dana melalui beberapa PTD Selain Bank/pengirim dana dengan tujuan penerima yang sama;
5. *Cuckoo Smurfing* yaitu upaya mengaburkan asal usul sumber dana dengan mengirimkan dana-dana dari hasil kejahatan melalui rekening pihak ketiga yang menunggu transfer dana dari luar negeri dan tidak menyadari bahwa dana yang diterimanya merupakan hasil tindak kejahatan;

6. Penggalangan dana secara digital, transfer, ataupun secara tunai dengan menyalahgunakan PTD Bukan Bank yang memiliki *global foreign branches* atau agen;

7. Penggunaan nama orang lain seperti saudara atau rekan lain yang menyebabkan proses deteksi cenderung sulit dilakukan;

8. Transaksi pengiriman dana dilakukan untuk menampung uang hasil kejahatan;

9. Transaksi dilakukan dengan menggunakan identitas palsu.

Lebih lanjut, berdasarkan hasil Survei Tipologi TPPU/TPPT/PPSPM yang dilakukan terhadap 48 (empat puluh delapan) sampel PTD Selain Bank yang berada di bawah pengaturan dan pengawasan Bank Indonesia, diperoleh tingkat risiko tipologi TPPT pada PTD Selain Bank berdasarkan persepsi penyelenggara sebagai berikut:

Tabel 3.15. Tingkat Risiko Tipologi TPPT pada PTD Bukan Bank

Tipologi TPPT	Tingkat Risiko	Kategori Risiko
Pengumpulan Dana - Ilegal: Hasil Kejahatan Kriminal Lainnya	5.94	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Dokumen Identitas Palsu	5.94	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Perjalanan dari dan ke lokasi aksi terorisme	5.88	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Pembelian dan Perawatan Kendaraan atau Mesin	5.88	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Biaya Kurir (Pengiriman Pesan, Uang)	5.88	Menengah
Penggunaan Dana: Operasi Terorisme Luar Negeri - Perjalanan Pejuang Teroris Asing	5.88	Menengah
Penggunaan Dana: Pelatihan - Pembuatan Senjata dan Bahan Peledak	5.88	Menengah
Penggunaan Dana: Gaji dan Kompensasi Anggota Kelompok Terorisme - Gaji Pimpinan dan Anggota Kelompok	5.88	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Pembelian Senjata dan Bahan Peledak	5.81	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Biaya Hidup Dasar (Pangan, Papan, Biaya Medis)	5.81	Menengah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan dan Pemeliharaan akun di Media Sosial	5.81	Menengah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan dan Pemeliharaan Situs Web	5.75	Menengah
Penggunaan Dana: Pelatihan - Penggunaan Senjata dan Bahan Peledak	5.75	Menengah
Penggunaan Dana: Pelatihan - Ideologi	5.75	Menengah
Penggunaan Dana: Gaji dan Kompensasi Anggota Kelompok Terorisme - Santunan kepada Keluarga bagi Anggota yang Masuk Penjara atau Meninggal	5.75	Menengah
Pengumpulan Dana - Legal: Penyimpangan Pengumpulan Donasi Melalui Ormas	5.69	Menengah
Pemindahan Dana: Melalui Pembawaan Uang Tunai Lintas Batas	5.69	Menengah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan Majalah atau Koran	5.69	Menengah
Penggunaan Dana: Pelatihan - Komunikasi Rahasia/Sandi	5.69	Menengah
Pengumpulan Dana - Legal: Pendanaan *Crowdfunding*	5.63	Menengah
Pengumpulan Dana - Ilegal: Eksploitasi Sumber Daya Alam secara Ilegal	5.63	Menengah
Pengumpulan Dana - Ilegal: Penculikan dengan Tebusan	5.56	Menengah
Penggunaan Dana: Propaganda dan Perekrutan - Media Promosi Lainnya (televisi, radio)	5.56	Menengah

Tipologi TPPT	Tingkat Risiko	Kategori Risiko
Pengumpulan Dana - Ilegal: Pemerasan	5.50	Menengah
Pemindahan Dana: Melalui Penyedia Barang dan Jasa	5.50	Menengah
Penggunaan Dana: Pelatihan - Pelatihan *Virtual/Online*	5.50	Menengah
Pengumpulan Dana - Legal: Sponsor Pribadi (*Terrorist Financier/Fundraiser*)	5.44	Menengah
Pemindahan Dana: Melalui Penyedia Jasa Keuangan	5.38	Menengah
Pemindahan Dana: Menggunakan Metode Pembayaran Baru	5.31	Menengah
Pemindahan Dana: Melalui Profesi	5.13	Menengah
Pengumpulan Dana - Legal: Pendanaan Mandiri (Selain dari Usaha Bisnis)	5.06	Menengah
Pengumpulan Dana - Legal: Usaha Bisnis yang Sah	4.81	Rendah

Berdasarkan hasil survei, tipologi pendanaan terorisme pada PTD Selain Bank yang memiliki risiko tertinggi adalah Pengumpulan Dana Ilegal: Hasil Kejahatan Kriminal Lainnya, Penggunaan Dana: Operasi Terorisme Domestik–Dokumen Identitas Palsu, dan Penggunaan Dana: Operasi Terorisme Domestik–Perjalanan dari dan ke lokasi aksi terorisme.

Pengumpulan Dana–Ilegal: Hasil Kejahatan Kriminal Lainnya merupakan tipologi TPPT yang paling berisiko terjadi pada PTD selain Bank. Sebagaimana hasil analisis putusan pengadilan, terdapat potensi penggalangan dana secara digital, transfer, ataupun secara tunai dengan menyalahgunakan PTD Bukan Bank yang memiliki *global foreign branches* atau agen.

Sementara itu, risiko tipologi Penggunaan Dana: Operasi Terorisme Domestik: Dokumen Identitas Palsu sejalan dengan tingginya risiko penggunaan identitas palsu untuk melakukan transaksi di PTD Selain Bank. Karakteristik pengguna jasa dari PTD Selain Bank yang sebagian besar merupakan *walk in customer*, memberikan celah kerentanan pada proses identifikasi dan verifikasi pengguna jasa yang dilakukan penyelenggara.

Lebih lanjut, potensi risiko tipologi Penggunaan Dana: Operasi Terorisme Domestik – Perjalanan dari dan ke lokasi aksi terorisme terkonfirmasi melalui hasil analisis putusan pengadilan yang menunjukkan bahwa PTD Selain Bank rentan digunakan sebagai media pemindahan dana, khususnya dana-dana yang bersumber dari yurisdiksi lain (transaksi *incoming).* Dana yang ditransfer melalui PTD Selain Bank digunakan untuk pendanaan kegiatan terorisme di dalam negeri atau dengan tujuan untuk ditransfer ke negara lain yang rentan akan aksi terorisme.

3.2.3 Tipologi TPPU dan TPPT pada Uang Elektronik dan Dompet Elektronik Selain Bank

A. Tipologi TPPU pada Penyelenggara Uang Elektronik dan Dompet Elektronik Selain Bank

Beberapa modus TPPU yang menggunakan penyelenggara Uang Elektronik (UE) dan Dompet Elektronik (DE) Selain Bank yaitu:

1. Penggunaan identitas orang lain atau identitas palsu dalam pembukaan/ registrasi akun UE dan DE untuk mengaburkan identitas *Beneficial Owner*;
2. Membeli dan/atau menggunakan akun UE dan DE atas nama orang lain untuk mengaburkan identitas *Beneficial Owner*;
3. Penggunaan akun UE sebagai penampungan hasil tindak kejahatan;
4. Pengisian ulang (*Top Up*) menggunakan uang tunai untuk mengaburkan identitas Pengirim dana dan asal usul sumber dana;

5. Mengunakan fitur transfer dana dan/atau melakukan tarik tunai (*cash out*) untuk memindahkan saldo UE yang didapat dari hasil tindak kejahatan;

6. Pencurian identitas kartu kredit atau kartu debit untuk dihubungkan dengan akun UE dan DE milik pelaku kejahatan. Selanjutnya pelaku kejahatan melakukan transaksi dengan dana yang bersumber dari kartu kredit dan/atau kartu debit tersebut;

7. Tidak membayar tagihan pada saat jatuh tempo setelah menggunakan fitur pascabayar atau *post-paid* untuk melakukan transaksi;

8. Transaksi dalam jumlah relatif kecil, namun dilakukan dengan frekuensi yang tinggi (*structuring*);

9. Transaksi dilakukan dengan menggunakan beberapa akun UE dan DE Selain Bank (*smurfing*);

10. Penjual bekerjasama dengan pembeli melakukan transaksi fiktif dan/atau pencucian uang berbasis perdagangan (*Trade-Based Money Laundering*) menggunakan fitur *Purchase & Payment*;

11. Transaksi dilakukan dengan mentransfer sejumlah uang dalam jumlah kecil ke beberapa orang yang akan mendapatkan komisi jika mentransfer kembali ke orang lainnya (*money mules/straw account*);

12. Transaksi dana masuk yang diikuti dengan penarikan uang;

13. Transaksi dana masuk yang berasal dari beberapa orang dalam waktu yang relatif bersamaan.

Lebih lanjut, berdasarkan hasil Survei Tipologi TPPU/TPPT/PPSPM yang dilakukan terhadap 32 (tiga puluh dua) sampel penyelenggara UE dan DE Selain Bank yang berada di bawah pengaturan dan pengawasan Bank Indonesia, diperoleh tingkat risiko tipologi TPPU pada UE dan DE Selain Bank berdasarkan persepsi penyelenggara sebagai berikut:

Tabel 3.16. Tingkat Risiko Tipologi TPPU pada UE dan DE Selain Bank

Tipologi TPPU	Tingkat Risiko	Kategori Risiko
Penggunaan Identitas Palsu	5.72	Menengah
Smurfing	5.16	Menengah
Aktivitas Perjudian Online	5.16	Menengah
Structuring	5.06	Menengah
Pemanfaatan Perusahaan Cangkang *(Shell Companies)* terhadap Uang Hasil Tindak Pidana Perpajakan	5.06	Menengah
Penyelundupan Manusia	5.06	Menengah
Mingling	5.06	Menengah
Pertukaran Komoditas	5.06	Menengah
Trade Based Money Laundering dan *Transfer Pricing*	4.97	Rendah
Bank Ilegal/Pengiriman Dana Alternatif/Hawala	4.97	Rendah
Transfer *Cross Border*	4.97	Rendah
Pemanfaatan Mata Uang Virtual	4.88	Rendah
Pemanfaatan *Nominees, Trust*, Anggota Keluarga atau Pihak Ketiga	4.88	Rendah
Pemanfaatan *Offshore Banks*, Perusahaan Bisnis Internasional dan *Trust* Lepas Pantai	4.78	Rendah
Pemanfaatan Internet Enkripsi, Akses terhadap Identitas, Perbankan Internasional	4.78	Rendah

Tipologi TPPU	Tingkat Risiko	Kategori Risiko
Pemanfaatan Jasa Profesi	4.59	Rendah
Properti/*Real Estate*, termasuk peran agen Properti	4.59	Rendah
Pembelian Aset Berharga	4.50	Rendah
Penukaran Uang Asing	4.50	Rendah
Pemanfaatan Kartu Kredit, Cek, Surat Perjanjian Hutang	4.41	Rendah
Pemanfaatan Korporasi	4.31	Rendah
Pemanfaatan Inovasi Sistem Pembayaran	4.31	Rendah
Pemanfaatan Sektor Non Keuangan	4.31	Rendah
Investasi di Pasar Modal, Penggunaan Perantara	4.31	Rendah
Perdagangan Perhiasan dan Logam Mulia	4.13	Rendah

Berdasarkan hasil survei, tipologi pencucian uang pada layanan UE dan DE Selain Bank yang memiliki risiko tertinggi adalah penggunaan identitas palsu, *smurfing*, dan aktivitas perjudian *online*. Penggunaan identitas menjadi salah satu tipologi yang berisiko tinggi karena terdapat kemudahan dalam pembuatan dokumen palsu, serta adanya kerentanan pada proses identifikasi dan verifikasi pengguna jasa. Transaksi yang dilakukan tanpa tatap muka menimbulkan kerentanan dan potensi terhadap pemalsuan identitas pengguna jasa. Lebih lanjut, terdapat kerentanan pada proses *electronic customer due diligence* (e-CDD) misalnya apabila penyelenggara tidak mewajibkan penggunaan nomor ponsel terdaftar, foto kartu identifias, dan foto diri pengguna jasa. Kondisi dimana beberapa penyelenggara juga belum terkoneksi dengan Dukcapil atau sumber lainnya, memberikan kerentanan pada proses verifikasi pengguna jasa.

Smurfing menjadi salah satu yang berisiko tinggi pada layanan UE dan DE Selain Bank karena terdapat potensi kerentanan dari penyelenggara dalam melakukan pemantauan profil maupun transaksi pengguna jasa. Selain itu, pengiriman dana ke beberapa rekening yang dilakukan pada tipologi *smurfing* ini juga menyebabkan terjadinya kesulitan bagi penyelenggara dan otoritas terkait dalam mendeteksi transaksi keuangan yang dianggap mencurigakan. Di sisi lain, penyelenggara yang tidak melakukan penatausahaan dokumen transaksi dengan baik, menyebabkan sulit dan terbatasnya akses untuk mendeteksi rekam jejak transaksi pengguna jasa.

Aktivitas perjudian *online* juga menjadi salah satu tipologi yang berisiko tinggi pada layanan UE dan DE Selain Bank. Kerentanan pada pengawasan dan pendeteksian aktivitas perjudian *online* ilegal serta aliran dananya memberikan potensi risiko TPPU. Selain itu, maraknya pembayaran pada situs *online* yang menggunakan layanan UE dan DE Selain Bank memberikan potensi risiko aktivitas perjudian *online* yang memanfaatkan penyelenggara UE dan DE Selain Bank.

B. Tipologi TPPT pada Penyelenggara Uang Elektronik dan Dompet Elektronik Selain Bank

Beberapa modus TPPT yang menggunakan UE dan DE Selain Bank yaitu:

1. Penggunaan identitas orang lain atau identitas palsu dalam pembukaan/registrasi akun UE dan DE Selain Bank untuk mengaburkan identitas *Beneficial Owner*;

2. Penggunaan akun UE dan DE Selain Bank untuk menampung dana hasil penggalangan donasi menyimpang;

3. Penggunaan fitur transfer dana termasuk transaksi lintas batas dan/atau tarik tunai untuk memindahkan dana yang akan digunakan untuk membiayai kegiatan terorisme;

4. Penggunaan fitur *Purchase & Payment* untuk membeli komponen pembuatan bahan peledak dan membuat bom serta tiket transportasi dan akomodasi;

5. Transaksi dalam jumlah relatif kecil, namun dilakukan dengan frekuensi yang tinggi melalui beberapa akun, baik akun teregistrasi maupun yang tidak teregistrasi (*structuring*).

Lebih lanjut, berdasarkan hasil Survei Tipologi TPPU/TPPT/PPSPM yang dilakukan terhadap 32 (tiga puluh dua) sampel penyelenggara UE dan DE yang berada di bawah pengaturan dan pengawasan Bank Indonesia, diperoleh tingkat risiko tipologi TPPT pada UE dan DE Selain Bank berdasarkan persepsi penyelenggara sebagai berikut:

Tabel 3.17. Tingkat Risiko Tipologi TPPT pada UE dan DE Selain Bank

Tipologi TPPT	Tingkat Risiko	Kategori Risiko
Pengumpulan Dana - Ilegal: Penculikan dengan Tebusan	5.16	Menengah
Pengumpulan Dana - Ilegal: Hasil Kejahatan Kriminal Lainnya	5.16	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Perjalanan dari dan ke lokasi aksi terorisme	5.16	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Pembelian dan Perawatan Kendaraan atau Mesin	5.16	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Pembelian Senjata dan Bahan Peledak	5.16	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Dokumen Identitas Palsu	5.16	Menengah
Penggunaan Dana: Operasi Terorisme Luar Negeri - Perjalanan Pejuang Teroris Asing	5.16	Menengah
Penggunaan Dana: Pelatihan - Penggunaan Senjata dan Bahan Peledak	5.16	Menengah
Penggunaan Dana: Gaji dan Kompensasi Anggota Kelompok Terorisme - Gaji Pimpinan dan Anggota Kelompok	5.16	Menengah
Penggunaan Dana: Pelatihan - Pembuatan Senjata dan Bahan Peledak	5.06	Menengah
Pengumpulan Dana - Ilegal: Eksploitasi Sumber Daya Alam secara Ilegal	5.06	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Biaya Hidup Dasar (Pangan, Papan, Biaya Medis)	5.06	Menengah
Penggunaan Dana: Operasi Terorisme Domestik - Biaya Kurir (Pengiriman Pesan, Uang)	5.06	Menengah
Penggunaan Dana: Gaji dan Kompensasi Anggota Kelompok Terorisme - Santunan kepada Keluarga bagi Anggota yang Masuk Penjara atau Meninggal	5.06	Menengah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan dan Pemeliharaan akun di Media Sosial	4.97	Rendah
Pengumpulan Dana - Ilegal: Pemerasan	4.97	Rendah
Pengumpulan Dana - Legal: Sponsor Pribadi *(Terrorist Financier/Fundraiser)*	4.88	Rendah
Pemindahan Dana: Melalui Pembawaan Uang Tunai Lintas Batas	4.88	Rendah
Penggunaan Dana: Pelatihan - Ideologi	4.88	Rendah
Pengumpulan Dana - Legal: Penyimpangan Pengumpulan Donasi Melalui Ormas	4.78	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan Majalah atau Koran	4.78	Rendah

Tipologi TPPT	Tingkat Risiko	Kategori Risiko
Penggunaan Dana: Pelatihan - Komunikasi Rahasia/Sandi	4.78	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan dan Pemeliharaan Situs Web	4.69	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Media Promosi Lainnya (televisi, radio)	4.59	Rendah
Penggunaan Dana: Pelatihan - Pelatihan Virtual/Online	4.41	Rendah
Pemindahan Dana: Melalui Profesi	4.31	Rendah
Pengumpulan Dana - Legal: Pendanaan *Crowdfunding*	4.31	Rendah
Pemindahan Dana: Melalui Penyedia Jasa Keuangan	4.13	Rendah
Pemindahan Dana: Melalui Penyedia Barang dan Jasa	4.03	Rendah
Pemindahan Dana: Menggunakan Metode Pembayaran Baru	3.94	Rendah
Pengumpulan Dana - Legal: Pendanaan Mandiri (Selain dari Usaha Bisnis)	3.66	Rendah
Pengumpulan Dana - Legal: Usaha Bisnis yang Sah	3.66	Rendah

Berdasarkan hasil survei, tipologi pendanaan terorisme pada layanan UE dan DE Selain Bank yang memiliki risiko tertinggi adalah Pengumpulan Dana – Ilegal: Penculikan dengan Tebusan, Pengumpulan Dana – Ilegal: Hasil Kejahatan Kriminal Lainnya, dan Penggunaan Dana: Operasi Terorisme Domestik – Perjalanan dari dan ke lokasi aksi terorisme.

Pengumpulan Dana *(Collecting)* merupakan tipologi TPPT yang paling berisiko terjadi pada layanan UE dan DE Selain Bank. Kemudahan dalam penggunaan layanan UE dan DE Selain Bank diperkirakan menyebabkan penyelenggara UE dan DE Selain Bank rentan digunakan untuk pengumpulan dana aksi terorisme, misalnya melalui penggunaan fasilitas transfer dana. Selain itu, fasilitas *Top Up* juga rentan digunakan untuk pengumpulan dana, khususnya pada UE dan DE Selain Bank yang *unregistered*. Proses CDD yang kurang mendalam pada *unregistered customer* menyebabkan layanan UE dan DE Selain Bank rentan disalahgunakan sebagai media pendanaan terorisme.

Penggunaan Dana: Operasi Terorisme Domestik – Perjalanan dari dan ke lokasi aksi Terorisme juga merupakan salah satu tipologi TPPT pada layanan UE dan DE Selain Bank. Layanan UE dan DE Selain Bank yang mudah digunakan rentan untuk dimanfaatkan sebagai sarana untuk memindahkan dana. Dana yang ditransfer kemudian akan digunakan untuk pendanaan aksi terorisme di dalam negeri, ataupun akan ditransfer ke negara lain yang rentan aksi terorisme.

3.2.4 Tipologi TPPU dan TPPT pada APMK Selain Bank

A. Tipologi TPPU pada APMK Selain Bank

Beberapa modus TPPU yang menggunakan penyelenggara APMK Selain Bank yaitu:

1. Fisik APMK yang ringkas memungkinkan pembawaan dan penyalahgunaan APMK untuk mengakses dana di yurisdiksi lain;

2. Pemanfaatan internet enkripsi, akses terhadap identitas, dan perbankan internasional. Teknik ini dilakukan dengan menggunakan internet, seperti melakukan peretasan data/informasi atau penipuan dengan menggunakan alamat *e-mail* atau situs *web* palsu;

3. Pemanfaatan fasilitas kartu kredit atas nama orang lain untuk mengaburkan identitas *Beneficial Owner*;

4. Pembayaran tagihan pada saat jatuh tempo dilakukan oleh pihak lain untuk mengaburkan identitas *Beneficial Owner*;

5. Melakukan transaksi *purchase & payment,* serta tarik tunai (*cash out*) untuk memanfaatkan dana hasil kejahatan;

6. Transaksi dalam jumlah relatif kecil, namun dilakukan dengan frekuensi yang tinggi (*structuring*).

Lebih lanjut, berdasarkan hasil Survei Tipologi TPPU/TPPT/PPSPM yang dilakukan terhadap 3 (tiga) sampel penyelenggara APMK yang berada di bawah pengaturan dan pengawasan Bank Indonesia, diperoleh tingkat risiko tipologi TPPU pada APMK Selain Bank berdasarkan persepsi penyelenggara sebagai berikut:

Tabel 3.18. Tingkat Risiko Tipologi TPPU pada APMK Selain Bank

Tipologi TPPU	Tingkat Risiko	Kategori Risiko
Penggunaan Identitas Palsu	7.00	Menengah
Pemanfaatan Internet Enkripsi, Akses terhadap Identitas, Perbankan Internasional	7.00	Menengah
Pemanfaatan Kartu Kredit, Cek, Surat Perjanjian Hutang	7.00	Menengah
Pemanfaatan Jasa Profesi	6.00	Menengah
Pemanfaatan Inovasi Sistem Pembayaran	6.00	Menengah
Structuring	5.00	Rendah
Smurfing	5.00	Rendah
Pemanfaatan Korporasi	5.00	Rendah
Pemanfaatan Sektor Non Keuangan	5.00	Rendah
Pemanfaatan *Offshore Banks*, Perusahaan Bisnis Internasional dan *Trust* Lepas Pantai	5.00	Rendah
Pemanfaatan Mata Uang Virtual	5.00	Rendah
Trade Based Money Laundering dan *Transfer Pricing*	5.00	Rendah
Bank Ilegal/Pengiriman Dana Alternatif/Hawala	5.00	Rendah
Pemanfaatan Perusahaan Cangkang *(Shell Companies)* terhadap Uang Hasil Tindak Pidana Perpajakan	5.00	Rendah
Properti/*Real Estate*, termasuk peran agen Properti	5.00	Rendah
Penyelundupan Manusia	5.00	Rendah
Pemanfaatan *Nominees, Trust,* Anggota Keluarga atau Pihak Ketiga	5.00	Rendah
Aktivitas Perjudian *Online*	5.00	Rendah
Mingling	5.00	Rendah
Transfer *Cross Border*	5.00	Rendah
Pertukaran Komoditas	5.00	Rendah
Perdagangan Perhiasan dan Logam Mulia	5.00	Rendah
Pembelian Aset Berharga	5.00	Rendah
Investasi di Pasar Modal, Penggunaan Perantara	5.00	Rendah
Penukaran Uang Asing	5.00	Rendah

Berdasarkan hasil survei, tipologi pencucian uang pada APMK Selain Bank yang memiliki risiko tertinggi adalah penggunaan identitas palsu, pemanfaatan internet enkripsi, akses terhadap identitas, perbankan internasional, serta pemanfaatan kartu kredit, cek, surat perjanjian utang.

Penggunaan identitas palsu merupakan tipologi yang paling berisiko karena terdapat kerentanan berupa kemudahan dalam pembuatan dokumen identitas palsu. Dokumen identitas palsu tersebut selanjutnya digunakan untuk mengajukan fasilitas kartu kredit.

Pemanfaatan internet enkripsi, akses terhadap identitas, dan perbankan internasional menjadi salah satu tipologi TPPU pada APMK Selain Bank. Hal tersebut misalnya dilakukan melalui peretasan data/informasi atau penipuan dengan menggunakan alamat *e-mail* atau situs *web* palsu. Selanjutnya dana hasil kejahatan digunakan untuk pencucian uang. Sulitnya menentukan pihak yang menggunakan atau menjadi penerima manfaat dari kartu kredit, menyebabkan APMK Selain Bank rentan digunakan untuk pencucian uang.

B. Tipologi TPPT pada APMK Selain Bank

Beberapa modus TPPT yang menggunakan APMK Selain Bank yaitu:

1. Fisik APMK yang ringkas memungkinkan pembawaan dan penyalahgunaan APMK untuk mengakses dana di yurisdiksi lain;
2. Pemanfaatan internet enkripsi, akses terhadap identitas, dan perbankan internasional. Teknik ini dilakukan dengan menggunakan internet, seperti melakukan peretasan data/informasi atau penipuan dengan menggunakan alamat *e-mail* atau situs *web* palsu;
3. Pemanfaatan fasilitas kartu kredit atas nama orang lain untuk mengaburkan identitas *Beneficial Owner*;
4. Pembayaran tagihan pada saat jatuh tempo dilakukan oleh pihak lain untuk mengaburkan identitas *Beneficial Owner*;
5. Melakukan transaksi *purchase & payment,* serta tarik tunai (*cash out*) untuk memanfaatkan dana hasil kejahatan;
6. Transaksi dalam jumlah relatif kecil, namun dilakukan dengan frekuensi yang tinggi (*structuring*);
7. Transaksi pengumpulan/penggalanan dana untuk aksi terorisme menggunakan APMK;
8. Pemanfaatan dana dari fasilitas kartu kredit untuk pelaksanaan aksi, seperti untuk pembelian senjata atau bahan peledak, maupun untuk perjalanan ke lokasi aksi terorisme.

Lebih lanjut, berdasarkan hasil Survei Tipologi TPPU/TPPT/PPSPM yang dilakukan terhadap 3 (tiga) sampel penyelenggara APMK yang berada di bawah pengaturan dan pengawasan Bank Indonesia, diperoleh tingkat risiko tipologi TPPT pada APMK berdasarkan persepsi penyelenggara sebagai berikut:

Tabel 3.19. Tingkat Risiko Tipologi TPPT pada APMK Selain Bank

Tipologi TPPT	Tingkat Risiko	Kategori Risiko
Pengumpulan Dana - Legal: Sponsor Pribadi *(Terrorist Financier/ Fundraiser)*	5.00	Rendah
Pengumpulan Dana - Legal: Penyimpangan Pengumpulan Donasi Melalui Ormas	5.00	Rendah
Pengumpulan Dana - Legal: Pendanaan *Crowdfunding*	5.00	Rendah
Pengumpulan Dana - Ilegal: Pemerasan	5.00	Rendah
Pengumpulan Dana - Ilegal: Penculikan dengan Tebusan	5.00	Rendah
Pengumpulan Dana - Ilegal: Hasil Kejahatan Kriminal Lainnya	5.00	Rendah
Penggunaan Dana: Operasi Terorisme Domestik - Perjalanan dari dan ke lokasi aksi terorisme	5.00	Rendah
Penggunaan Dana: Operasi Terorisme Domestik - Pembelian dan Perawatan Kendaraan atau Mesin	5.00	Rendah
Penggunaan Dana: Operasi Terorisme Domestik - Dokumen Identitas Palsu	5.00	Rendah

Tipologi TPPT	Tingkat Risiko	Kategori Risiko
Penggunaan Dana: Operasi Terorisme Domestik - Biaya Hidup Dasar (Pangan, Papan, Biaya Medis)	5.00	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan dan Pemeliharaan akun di Media Sosial	5.00	Rendah
Penggunaan Dana: Pelatihan - Penggunaan Senjata dan Bahan Peledak	5.00	Rendah
Penggunaan Dana: Pelatihan - Pembuatan Senjata dan Bahan Peledak	5.00	Rendah
Penggunaan Dana: Pelatihan - Komunikasi Rahasia/Sandi	5.00	Rendah
Pengumpulan Dana - Legal: Usaha Bisnis yang Sah	4.00	Rendah
Pengumpulan Dana - Legal: Pendanaan Mandiri (Selain dari Usaha Bisnis)	4.00	Rendah
Pengumpulan Dana - Ilegal: Eksploitasi Sumber Daya Alam secara Ilegal	4.00	Rendah
Pemindahan Dana: Melalui Penyedia Jasa Keuangan	4.00	Rendah
Pemindahan Dana: Melalui Pembawaan Uang Tunai Lintas Batas	4.00	Rendah
Pemindahan Dana: Menggunakan Metode Pembayaran Baru	4.00	Rendah
Penggunaan Dana: Operasi Terorisme Luar Negeri - Perjalanan Pejuang Teroris Asing	4.00	Rendah
Penggunaan Dana: Pelatihan - Ideologi	4.00	Rendah
Penggunaan Dana: Pelatihan - Pelatihan *Virtual/Online*	4.00	Rendah
Penggunaan Dana: Gaji dan Kompensasi Anggota Kelompok Terorisme - Gaji Pimpinan dan Anggota Kelompok	4.00	Rendah
Pemindahan Dana: Melalui Penyedia Barang dan Jasa	3.00	Rendah
Pemindahan Dana: Melalui Profesi	3.00	Rendah
Penggunaan Dana: Operasi Terorisme Domestik - Pembelian Senjata dan Bahan Peledak	3.00	Rendah
Penggunaan Dana: Operasi Terorisme Domestik - Biaya Kurir (Pengiriman Pesan, Uang)	3.00	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan Majalah atau Koran	3.00	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Pembuatan dan Pemeliharaan Situs Web	3.00	Rendah
Penggunaan Dana: Propaganda dan Perekrutan - Media Promosi Lainnya (televisi, radio)	3.00	Rendah
Penggunaan Dana: Gaji dan Kompensasi Anggota Kelompok Terorisme - Santunan kepada Keluarga bagi Anggota yang Masuk Penjara atau Meninggal	3.00	Rendah

Berdasarkan hasil survei, tipologi pendanaan terorisme pada penyelenggara APMK Selain Bank yang memiliki risiko yang cenderung lebih tinggi adalah Pengumpulan Dana - Legal: Sponsor Pribadi *(Terrorist Financier/ Fundraiser)*, Pengumpulan Dana - Legal: Penyimpangan Pengumpulan Donasi Melalui Ormas, Pengumpulan Dana - Legal: Pendanaan *Crowdfunding*.

Tahap Pengumpulan Dana *(Collecting)* merupakan tipologi TPPT yang paling berisiko pada penyelenggara APMK Selain Bank. Sebagaimana analisis hasil putusan pengadilan, pada tahap pengumpulan dana *(collecting)*, terdapat potensi pengumpulan dana yang bersumber dari simpatisan dan anggota kelompok dari kelompok teror. Dalam hal ini, dana pada fasilitas kartu kredit rentan dimanfaatkan untuk mendanai kegiatan terorisme oleh pemilik kartu kredit, baik pendanaan sebagai sponsor pribadi, pendanaan melalui donasi, maupun melalui pendanaan *crowdfunding*.

3.2.5 Tipologi PPSPM

Berdasarkan data hasil putusan pengadilan selama periode tahun 2015-2020, belum ditemukan adanya kasus PPSPM. Selain itu, berdasarkan hasil survei juga tidak ditemukan adanya pengalaman praktik PPSPM pada PJP Lembaga Selain Bank dan KUPVA Bukan Bank di bawah pengaturan dan pengawasan Bank Indonesia.

Namun demikian, berdasarkan NRA TPPT/PPSPM Tahun 2021, potensi ancaman PPSPM di Indonesia diantaranya berasal dari:

1. Transaksi perdagangan yang dilakukan dengan pihak-pihak yang berasal dari negara-negara yang berisiko tinggi berdasarkan Resolusi Dewan Keamanan PBB; serta

2. Penyalahgunaan rekening WNA yang berasal dari negara yang berisiko tinggi berdasarkan Resolusi Dewan Keamanan PBB, yang sudah tidak tinggal/bekerja di Indonesia.

Sementara itu, berdasarkan laporan *Guidance on Proliferation Financing Risk Asessment and Mitigation* yang diterbitkan oleh FATF pada Juni 2021, terdapat beberapa indikator risiko PPSPM pada profil Pengguna Jasa, yaitu:

1. Pengguna Jasa yang enggan melengkapi informasi tambahan terkait aktivitas transaksi perdagangan yang dilakukan;

2. Berdasarkan temuan pada proses CDD, Pengguna Jasa dan/atau entitas dagang, termasuk pemilik atau pimpinan badan usaha, diketahui terdaftar dalam daftar pendanaan proliferasi senjata pemusnah massal;

3. Pengguna Jasa yang memiliki hubungan usaha dengan negara yang terkena sanksi Dewan Keamanan PBB atau dinilai memiliki tingkat risiko PPSPM yang tinggi berdasarkan sumber informasi terkini yang dapat dipercaya dan independen termasuk Penilaian Risiko Nasional;

4. Pengguna Jasa yang terlibat dengan aktivitas transaksi perdagangan *dual-use goods* dan/atau barang-barang eskpor dan/atau peralatan kompleks namun tidak sesuai dengan latar belakang atau profil usaha Pengguna Jasa;

5. Pengguna Jasa yang aktivitas perdagangannya banyak melibatkan pihak ketiga dengan lini bisnis yang tidak sesuai dengan profil usaha Pengguna Jasa;

6. Pengguna Jasa yang melakukan transaksi pemindahan dana dengan volume yang sangat tinggi dengan profil usaha yang tidak jelas. Pada beberapa kasus, kegiatan pemindahan dana dilakukan oleh Badan Usaha yang terlibat dengan Proliferasi Program yang disponsori oleh suatu negara, dengan profil penerima dananya merupakan perusahaan manufaktur atau jasa pengiriman ekspor;

7. Pengguna Jasa yang terafiliasi dengan Universitas atau Institusi Penelitian yang terlibat dengan perdagangan *dual-use goods* dan/atau barang-barang eskpor.

Selanjutnya, diketahui juga beberapa indikator risiko PPSM pada kegiatan transaksi sebagai berikut:

1. Pengirim dan/atau Penerima dana merupakan orang atau entitas yang berdomisili atau berasal dari negara yang terkena sanksi Dewan Keamanan PBB atau dinilai memiliki tingkat risiko PPSPM yang tinggi berdasarkan sumber informasi terkini yang dapat dipercaya dan independen termasuk Penilaian Risiko Nasional;

2. Pemilik akun melakukan transaksi yang melibatkan barang-barang yang diatur dibawah pengaturan *dual-use goods* dan/atau pengaturan kontrol ekspor, atau pemilik akun diketahui pernah melanggar peraturan pada pengaturan *dual-use goods* dan/atau kontrol ekspor;

3. Transaksi yang melibatkan perusahaan dengan struktur kepemilikan yang kurang jelas serta terindikasi merupakan perusahaan cangkang (*shell companies*);

4. Transaksi antar perusahaan yang memiliki hubungan seperti satu kepemilikan, satu alamat, satu nomor kontak, atau kegiatan bisnis yang mirip;

5. Pemilik akun melalukan transaksi dengan sikap yang berbelit-belit;

6. Transaksi yang dilakukan oleh Pengirim dan/ atau Penerima yang memiliki kaitan dengan jasa keuangan yang berada atau memiliki cabang di negara yang terkena sanksi Dewan Keamanan PBB atau dinilai memiliki tingkat risiko PPSPM yang tinggi berdasarkan sumber informasi terkini yang dapat dipercaya dan *independent* termasuk Penilaian Risiko Nasional;

7. Transaksi perdagangan yang dilakukan dengan menggunakan uang tunai.

Selain itu, Produk dan Layanan yang rentan digunakan sebagai media PPSPM adalah Produk dan Layanan yang memfasilitasi transaksi *cross-border* dan/atau Produk dan Layanan yang dapat di akses di berbagai yurisdiksi. Adapun risiko *delivery channel* perlu dipertimbangkan oleh Penyelenggara yang memiliki cabang dan/atau mitra di berbagai yurisdiksi.

Lebih lanjut, beberapa tipologi PPSPM lainnya yang bersumber dari berbagai literatur diantaranya yaitu:

1. Transaksi menggunakan identitas palsu;

2. Transaksi menggunakan dokumen fiktif atau tidak valid;

3. Transaksi tidak sesuai profil pengguna jasa;

4. Transaksi menggunakan informasi fiktif terkait lokasi pengiriman;

5. Pengguna jasa memberikan informasi yang tidak valid, terutama yang berkaitan dengan barang atau jasa yang diekspor;

6. Transaksi tanpa disertai dengan dokumen pendukung, seperti faktur atau rincian lainnya;

7. Pengguna jasa tidak memberikan informasi secara jelas dan valid, serta menolak untuk memberikan informasi tambahan;

8. Adanya transaksi pengiriman uang yang diikuti dengan penarikan secara tunai dalam rentang waktu yang relatif singkat;

9. Transaksi menggunakan rekening pribadi atau perusahaan;

10. Penggunaan perusahaan cangkang;

11. Penggunaan *front company*;

12. Transaksi melibatkan negara yang rentan terhadap aktivitas proliferasi;

13. Transaksi melibatkan orang atau entitas dari luar negeri yang ditujukan untuk menyamarkan aliran dana;

14. Transaksi melibatkan perusahaan pengiriman barang;

15. Transaksi melibatkan perusahaan ekspor-impor;

16. Transaksi pemesanan barang dilakukan oleh orang atau perusahaan dari luar negeri;

17. Transaksi melibatkan pengiriman barang yang tidak sesuai dengan profil negara. Misalnya, peralatan manufaktur semikonduktor dikirim ke negara yang tidak memiliki industri elektronik;

18. Terdapat hubungan diantara perusahaan yang saling melakukan pengiriman barang, yaitu memiliki pemilik atau manajemen perusahaan yang sama;

19. Rute pengiriman yang berputar;

20. Transaksi melibatkan rute pengiriman ke negara dengan hukum ekspor-impor yang lemah;
21. Transaksi melibatkan pengiriman barang yang tidak sesuai dengan pola perdagangan pada umumnya;
22. Transaksi melibatkan lembaga keuangan yang memiliki pengawasan APU PPT yang lemah atau pada negara dengan hukum yang lemah;
23. Transaksi dengan nilai biaya pengiriman yang rendah;
24. Informasi yang tidak konsisten pada dokumen keuangan dan arus keuangan;
25. Transaksi menggunakan *wire transfer*;
26. Pola aktivitas *wire transfer* yang tidak biasa atau tidak memiliki tujuan yang jelas;
27. Pengguna baru meminta melakukan transaksi *Letter of Credit*;
28. Adanya instruksi untuk melakukan pembayaran yang berasal atau kepada pihak tertentu yang tidak disebutkan dalam dokumen;
29. Transaksi yang melibatkan barang-barang yang dikendalikan dalam rezim kontrol ekspor PPSPM;
30. Transaksi yang melibatkan seseorang atau entitas yang memiliki hubungan dengan negara yang rentan dengan praktik PPSPM;
31. Transaksi yang melibatkan seseorang atau entitas dari negara yang rentan dengan praktik PPSPM;
32. Transaksi yang menggunakan uang tunai atau logam mulia;
33. Keterlibatan perusahaan perdagangan kecil atau perusahaan perantara yang melakukan kegiatan bisnis tidak sesuai dengan kegiatan usahanya;
34. Perusahaan yang melakukan transaksi pengiriman uang secara ilegal;
35. Transaksi yang dilakukan antar perusahaan;
36. Terdapat hubungan antara pengguna jasa dengan rekannya, yaitu misalnya memiliki alamat tempat tinggal, alamat IP, atau nomor telepon yang sama;
37. Transaksi yang melibatkan universitas di negara rentan praktik proliferasi;
38. Transaksi pembelian barang-barang industri yang menggunakan rekening pribadi;
39. Pengguna jasa termasuk dalam daftar negatif atau daftar orang yang melakukan tindakan kriminal, serta ditolak untuk melakukan kegiatan ekspor;
40. Pengguna jasa terlibat dalam transaksi perdagangan yang kompleks, serta melibatkan banyak perantara dan pihak ketiga dalam kegiatan usaha yang tidak sesuai dengan profil usahanya.
41. Penerima manfaat berdomisili di negara yang rentan aktivitas proliferasi;
42. Transaksi yang menggunakan atau melibatkan perusahaan dengan struktur kepemilikan yang tidak jelas;
43. Transaksi dengan menggunakan uang tunai yang dilakukan oleh perusahaan manufaktur atau perusahaan yang bergerak pada bidang perdagangan;
44. Transaksi yang memiliki lokasi tujuan pengiriman yang berbeda dengan lokasi importir;
45. Pembayaran transaksi impor yang dilakukan oleh entitas lain.

3.3 Kasus TPPU, TPPT, dan PPSPM

3.3.1 Kasus TPPU

A. Kasus TPPU pada KUPVA Bukan Bank

1. Kasus DY (Putusan Nomor 57/Pid. Sus/2019/PT.DKI)

DY merupakan pemilik dari PT PSS dan PT UJS, serta beberapa perusahaan lain yaitu PT HC, PT GU, PT DUV, dan PT DRS. Perusahaan-perusahaan yang dimiliki DY ini adalah perusahaan yang bergerak di bidang *supplier, trading,* dan investasi. Namun, dalam praktiknya perusahaan-perusahaan tersebut hanya melakukan Kegiatan Usaha Penukaran Valuta Asing (KUPVA) atau *money changer*. Dalam melakukan transaksi usaha *money changer*, DY menggunakan beberapa rekening atas nama sendiri ataupun atas nama karyawannya. DY dalam menjalankan usahanya dibantu oleh FHP selaku Direktur dari PT PSS dan HR selaku Direktur PT UJS. Meskipun demikian, keduanya tidak melakukan tugas dan peran sesuai dengan jabatannya.

Melalui kegiatan usaha yang dilakukan, DY melakukan pengiriman uang ke luar negeri dengan melampirkan *invoice* fiktif dengan berkedok *money changer* ilegal. Pengiriman uang telah dilakukan ke berbagai negara, seperti Tiongkok, India, Jepang, Jerman, dan Australia. Pengiriman uang tersebut dilakukan melalui perbankan, dengan menggunakan beberapa rekening atas nama DY dan karyawannya. Tidak hanya itu, DY dan karyawannya juga melakukan pembukaan akun rekening di luar negeri yang selanjutnya rekening tersebut digunakan untuk menerima hasil tindak pidana. Kegiatan *money changer* yang dilakukan DY digunakan untuk menerima uang dari pelaku jaringan narkotika. Selain itu, kegiatan ketiga perusahaan DY, yaitu PT PSS, PT UJS, dan PT HC juga memiliki keterlibatan dengan pencucian uang, yakni terkait kasus judi *online*.

Pada kasus DY terdapat beberapa transaksi pada perusahaan yang melakukan aktivitas *money changer* ilegal dalam kaitannya dengan pencucian uang hasil narkotika. Beberapa transaksi yang berkaitan dengan aktivitas *money changer* ilegal tersebut antara lain:

1. Menerima pentransferan dana dari AM (*money changer* ilegal) sebesar Rp1.546.462.000,00 yang kemudian dikirim ke China.

2. Menerima pentransferan dana dari LK sebesar Rp8.520.055.000,00 dalam rangka penukaran valas, yang kemudian dikirim ke luar negeri dengan melampirkan *invoice* fiktif.

3. Menerima pentransferan dana sebesar Rp15.000.000,00 dari PT DUV dalam rangka memindahkan dana ke rekening lain yang dikuasai DY.

4. DY melakukan pentransferan ke rekening LT (mantan Direktur PT DUV) sebesar Rp267.531.368.888,00. Dalam hal ini, rekening LT termasuk rekening yang dikuasai DY.

Tipologi Pencucian Uang

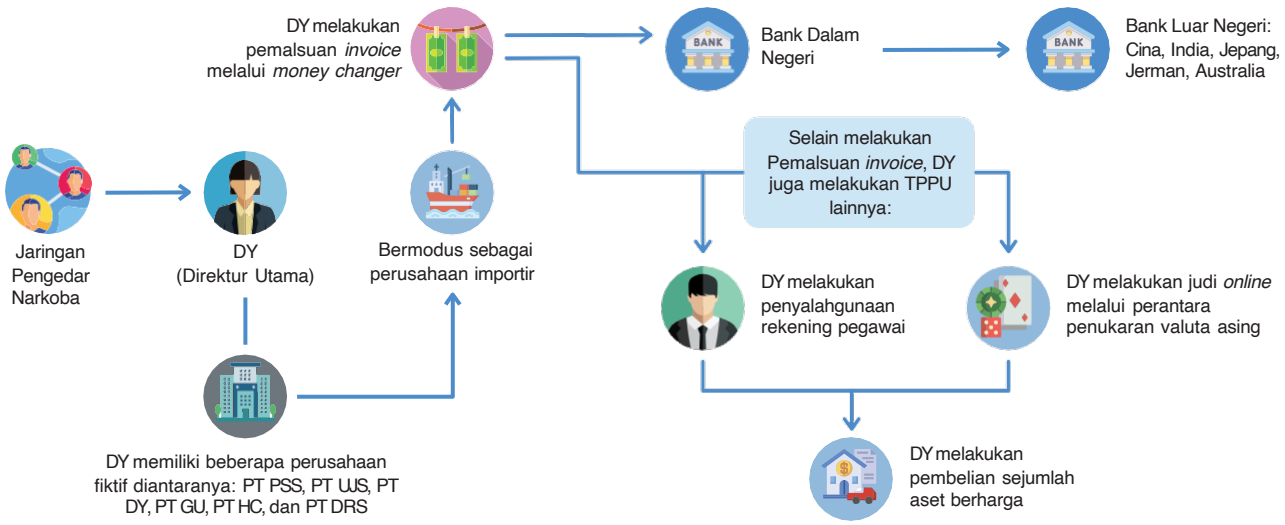
1. Mendirikan perusahaan dan membuat rekening atas nama perusahaan yang digunakan untuk menampung uang hasil kejahatan dengan memberikan keterangan palsu.

2. Penggunaan beberapa rekening atas nama sendiri ataupun atas nama karyawan dalam melakukan transaksi.

3. Transaksi dalam frekuensi dan nominal yang besar.

Skema Pencucian Uang

Gambar 3.1. Skema Kasus DY



Sumber: NRA TPPU Tahun 2021

Red Flag

1. Perusahaan menjalankan usaha tidak sesuai dengan bidang usahanya, yaitu menjalankan KUPVA tidak berizin.

2. Penggunaan beberapa rekening atas nama sendiri ataupun atas nama karyawan dalam melakukan transaksi.

3. Transaksi dalam frekuensi dan nominal yang besar.

2. Kasus NL (Putusan Nomor 318/Pid.Sus/2019/PN.Tng)

NL merupakan pegawai pada *Money Changer* PT MIV dan PT TV milik AH. PT TV dan PT MIV dalam melakukan transaksi, menggunakan beberapa rekening dari berbagai bank yang menggunakan nama NL, nama perusahaan, maupun orang lain. Rekening tersebut digunakan untuk menerima dan melakukan transaksi dari sindikat peredaran narkotika. Selain itu, rekening-rekening ini juga digunakan untuk memindahkan dana dari rekening satu ke rekening lainnya, serta digunakan untuk pengiriman dana ke luar negeri. Aktivitas memindah-mindahkan dana dari rekening satu ke rekening lainnya ini dilakukan oleh NL dengan alasan untuk penukaran uang. Kemudian, selain PT MIV dan PT TV, terdapat juga PT SIV. Diketahuinya kasus pencucian uang yang dilakukan oleh NL ini, berawal dari penangkapan NL di Kantor Bea Cukai Bandara Soekarno Hatta. Pada saat itu, NL baru kembali dari Singapura dengan alasan berobat. Namun, didapatkan bahwa NL membawa masuk uang tunai pecahan Dollar Singapura dengan pecahan SGD 1.000 sebanyak 2.166 lembar ke Indonesia. Uang tersebut ditempatkan di dalam koper, yang awalnya dikatakan bahwa koper tersebut berisi buku. Selama melakukan aktivitas pencucian uang ini, NL dan AH telah mendapatkan keuntungan, yaitu uang yang masih dalam rekening dan aset-aset yang telah dibeli dengan uang hasil narkotika.

Pada kasus NL, terdapat beberapa transaksi dimana NL telah menerima uang hasil pencucian uang dengan tindak pidana asal narkotika. Pemindahan dana dilakukan melalui rekening yang dikuasainya, baik atas nama NL, atas nama perusahaan *money changer*, maupun atas nama orang lain, diantaranya yaitu:

1. Menerima pengiriman dana dari FS sebesar Rp645.961.975,00.

2. Menerima pengiriman dana dari PC sebesar Rp2.174.680.000,00.
3. Menerima pengiriman dana dari LB sebesar Rp4296.722.000,00.
4. Menerima pengiriman dana dari MN, CV CM, sebesar Rp7.843.250.000,00.
5. Menerima pengiriman dana dari PT SIJ sebesar Rp629.600.000,00.
6. Menerima pengiriman dana dari HB sebesar Rp197.500.000,00.
7. Menerima pengiriman dana dari FS sebesar Rp3.251.291.458,00.

Tipologi Pencucian Uang

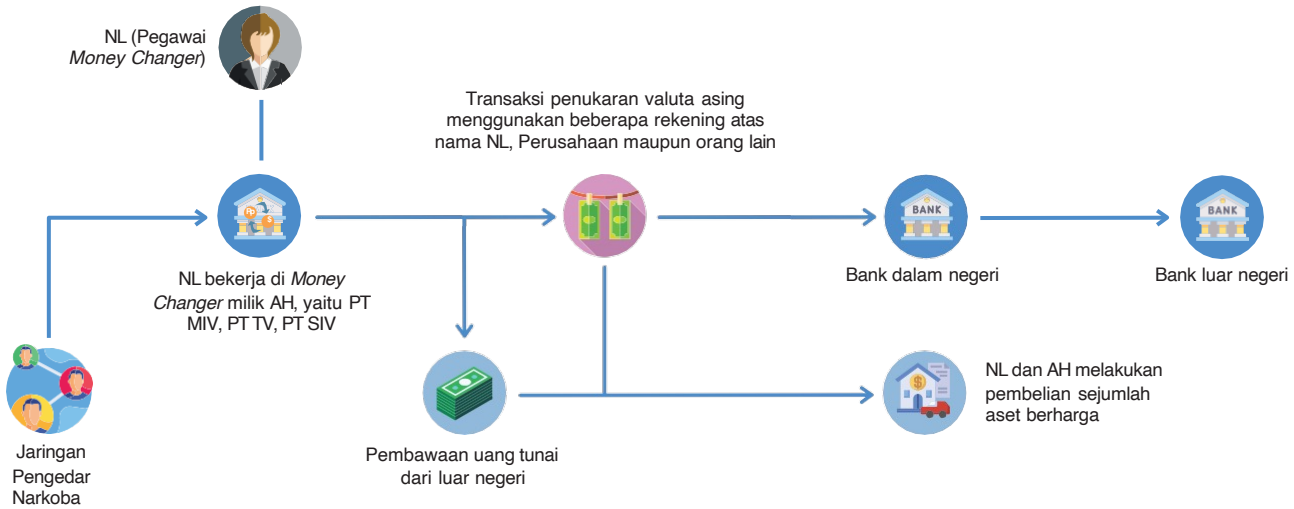
1. Mendirikan perusahaan dan membuat rekening atas nama perusahaan yang digunakan sebagai tempat untuk menampung uang hasil kejahatan.
2. Menggunakan beberapa rekening atas nama pribadi, perusahaan, maupun orang lain dalam melakukan transaksi.
3. Pengiriman uang ke luar negeri dalam jumlah besar.
4. Transaksi penukaran UKA dalam jumlah besar.
5. Aktivitas memindah-mindahkan uang dari rekening satu ke rekening lainnya.
6. Dana hasil pencucian uang dicampur dengan uang dari kegiatan usaha jual beli valas *(mingling)* untuk menyamarkan asal usul dana.

Red Flag

1. Perusahaan menggunakan beberapa rekening atas nama pribadi, perusahaan, maupun orang lain dalam menjalankan kegiatan usahanya.
2. Adanya aktivitas memindah-mindahkan uang dari satu rekening ke rekening lainnya.
3. Adanya pembawaan uang tunai pecahan Dollar Singapura dengan pecahan SGD 1.000 sebanyak 2.166 lembar ke Indonesia.

Skema Pencucian Uang

Gambar 3.2. Skema Kasus NL



B. Kasus TPPU pada PTD Selain Bank

1. EA (Putusan Nomor 1106/Pid.Sus/2019/PN.Jkt.Utr)

EA melakukan pembuatan KTP palsu yang akan digunakan untuk membuka rekening bank. Dalam hal ini, EA memerintahkan sopirnya yaitu DN untuk membuat KTP palsu dengan menggunakan foto AKN. Kemudian, DN membuat 2 (dua) buah KTP palsu tersebut atas nama RS dan MIR. Kedua KTP ini selanjutnya diberikan kepada AKN untuk dibuatkan beberapa rekening yang nantinya akan diberikan kepada EA. Sebelumnya, EA juga telah menggunakan KTP palsu atas nama YL untuk membuat rekening bank. Rekening-rekening bank yang telah dibuat EA ini akan diberikan kepada IG (WNA Nigeria). Sehubungan dengan aktivitas ini, EA telah memiliki 13 (tiga belas) rekening di beberapa bank untuk menerima dana dari IG.

EA selanjutnya melakukan pencairan dana yang diterima dari IG melalui PTD Selain Bank menggunakan KTP atas nama EA dan rekannya, yaitu TA dan NA. Dana yang diterima oleh EA merupakan hasil tindak pidana penipuan yang dilakukan oleh DM (WNA Nigeria). Atas penerimaan dana ini, EA akan mendapatkan komisi sebesar 3% dari setiap dana masuk. Selain itu, dana yang diperoleh dari transaksi-transaksi tersebut, telah digunakan EA untuk membeli berbagai aset dan keperluan pribadi.

Pada kasus EA ini, diketahui terdapat beberapa transaksi yang dilakukan melalui rekening bank maupun PTD Selain Bank.

Adapun jumlah transaksi yang melibatkan PTD Selain Bank pada periode 2 Juni 2016 hingga 21 Agustus 2017 adalah sebesar Rp1.942.313.258,70, dengan rincian sebagai berikut:

1. BRI: Rp135.344.500,00
2. NA: Rp816.145.058,70
3. EA: Rp354.826.700,00
4. MR: Rp135.040.000,00
5. YL: Rp500.957.000,00

Tipologi Pencucian Uang

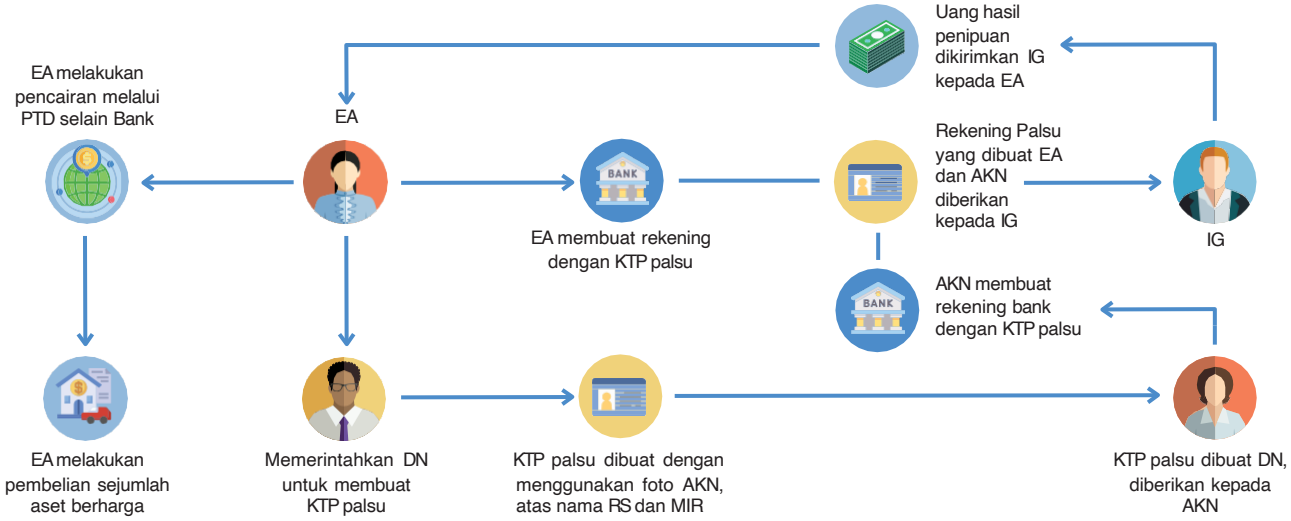
1. Menggunakan identitas palsu dalam pembuatan rekening.
2. Menggunakan beberapa rekening baik atas nama pribadi, maupun nama palsu untuk menampung hasil kejahatan.
3. Penggunaan identitas palsu dalam melakukan transaksi di PTD Selain Bank.

Red Flag

1. Pembuatan KTP palsu untuk membuka rekening bank.
2. Menggunakan beberapa rekening dari berbagai bank untuk menerima transaksi dari luar negeri.
3. Transaksi dalam jumlah besar.

Skema Pencucian Uang

Gambar 3.3. Skema Kasus EA



2. PB dan CPM (Putusan Nomor 23/Pid. Sus/2020/PN.Jkt.Pst)

Pada awalnya AMM yang berkedudukan di Jerman, ingin melakukan transaksi ilegal secara *online* dengan menggunakan mesin EDC. Sehubungan dengan hal tersebut, AMM meminta bantuan kepada CPM yang berlokasi di Indonesia. Selanjutnya, CPM menghubungi rekannya PB untuk membantu AMM. PB tidak memiliki mesin EDC, namun memiliki *website* X yang dapat digunakan untuk bertransaksi. Setelah melakukan pembicaraan antara AMM dan PB, maka disepakati bahwa AMM akan menggunakan *website* milik PB untuk melakukan transaksi dengan kartu kredit secara *online*. Selain itu, juga disepakati mengenai pembagian hasil atas keuntungan yang didapat yaitu 20% untuk PB, 10% untuk CPM dan rekan, serta 70% untuk AMM.

Transaksi yang dilakukan AMM dan PB ini merupakan transaksi fiktif yang dilakukan untuk mendapatkan uang tanpa harus menerima barang yang ditransaksikan. Dalam hal ini, jika uang sudah ditransfer oleh Bank ke rekening milik PB, maka PB tidak harus mengirim barang ke AMM. Dari transaksi tersebut, uang bagian AMM akan dikirimkan oleh PB melalui PTD Selain Bank. Pada suatu waktu, terjadi kesalahan huruf dalam transaksi menggunakan PTD Selain Bank sehingga uang dikembalikan secara tunai dan dipotong biaya administrasi sebesar Rp2.000.000,00. Karena kejadian tersebut, AMM menganggap PTD Selain Bank tidak praktis, sehingga AMM meminta CPM untuk mengirimkan uang menggunakan *bitcoin*. Sejak saat itu, setiap AMM melakukan transaksi di *website* X, maka uang atas transaksi yang dilakukan itu akan dikirim ke rekening Bank A atas nama PB. Lalu, oleh PB akan ditransfer ke rekening Bank A atas nama SS. Kemudian, uang tersebut akan dikirimkan oleh LSD kepada AMM melalui *account bitcoin* milik SS. Atas kerja sama transaksi fiktif ini, PB, CPM, dan rekan- rekannya telah mendapatkan keuntungan dan menggunakan keuntungan tersebut untuk membeli beberapa aset dan kepentingan pribadi.

Pada kasus ini terdapat beberapa transaksi yang melibatkan PTD Selain Bank, diantaranya:

1. Pada tanggal 11 Maret 2019, pengiriman uang kepada AMM sebesar Rp135.000.000,00;

2. Pada tanggal 12 Maret 2019, pengiriman uang kepada AMM sebesar Rp153.000.000,00 (Transaksi gagal dikarenakan adanya kesalahan huruf).

Tipologi Pencucian Uang

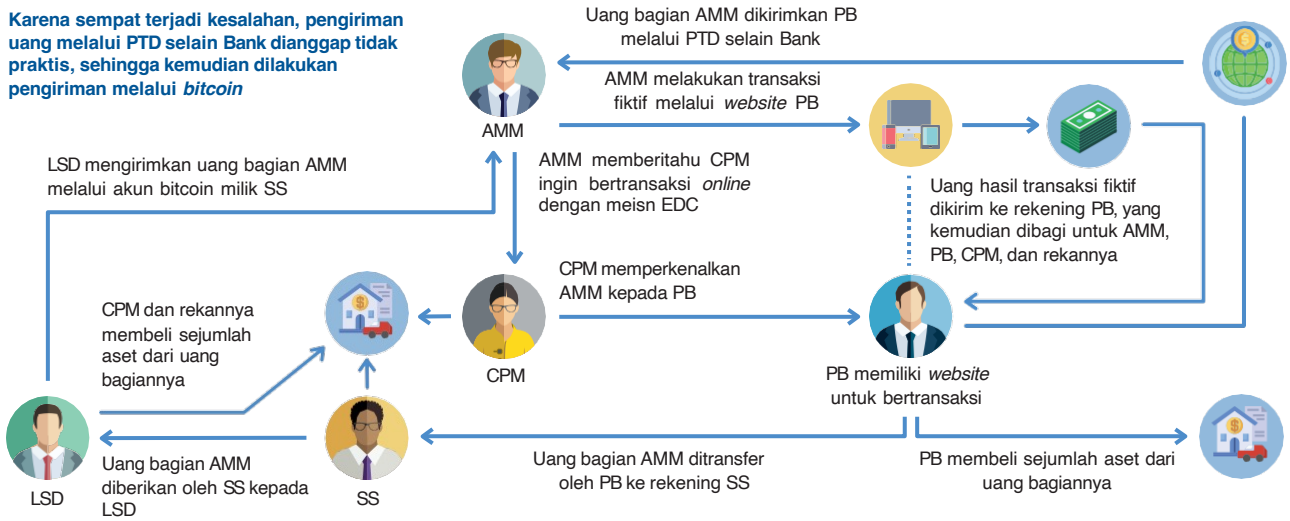
1. Adanya aktivitas memindah-mindahkan uang dari rekening satu ke rekening lainnya.
2. Transaksi yang dilakukan adalah transaksi fiktif, dengan tidak adanya pengiriman barang atas transaksi yang dilakukan.

Red Flag

1. Melakukan transaksi dalam jumlah yang besar dan dalam waktu berdekatan.
2. Adanya aktivitas memindah-mindahkan uang dari rekening satu ke rekening lainnya.

Skema Pencucian Uang

Gambar 3.4. Skema Kasus PB dan CPM



3.3.2 Kasus TPPT

A. Kasus TPPT pada KUPVA Bukan Bank

MI (Putusan Nomor 263/Pid.Sus/2020/PN.Jkt.Tim)

MI bersama rekannya berangkat ke Suriah dan bergabung dalam kelompok DI. Dalam rangka persiapan teknis, MI melakukan penarikan uang tunai sebesar Rp50.000.000,00 di salah satu bank di Aceh. Selanjutnya, uang tersebut ditukar di salah satu *money changer*. Lalu, MI juga menerima transfer uang sebesar Rp100.000.000,00 melalui bank, yang kemudian ditukarkan dalam bentuk USD. MI juga menggunakan layanan transfer bank melalui rekening milik istri dari salah satu rekannya untuk melakukan pembelian tiket pesawat ke Afghanistan sebesar Rp120.000.000,00. Pembelian tiket ini dilakukan dengan menggunakan uang rekannya terlebih dahulu yang kemudian akan diganti dengan uang hasil pengumpulan dari peserta jihad.

Tipologi Pendanaan Terorisme

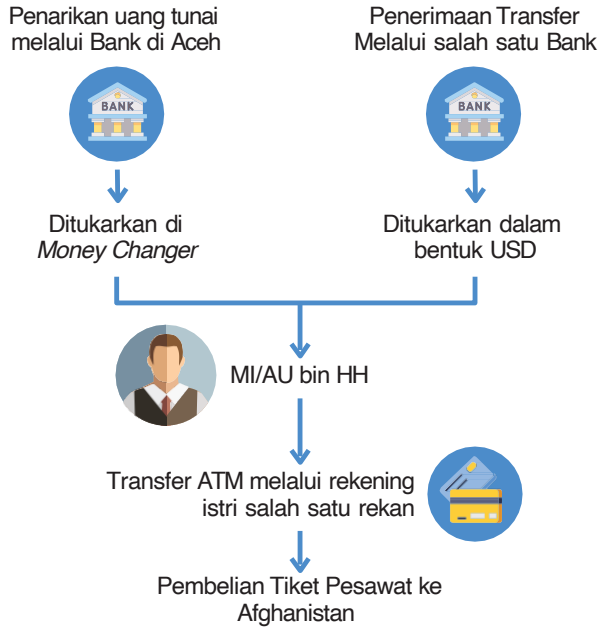
1. Penggunaan dana - untuk operasi terorisme ke luar negeri
2. Pemindahan dana - melalui penyedia jasa keuangan

Red Flag

1. Penarikan uang tunai dalam jumlah besar, yang tidak sesuai dengan riwayat transaksi dan profil pengguna jasa.
2. Penerimaan uang yang diikuti dengan penarikan uang tunai.
3. Penukaran USD dalam jumlah besar.

Skema Pendanaan Terorisme

Gambar 3.5. Skema Kasus MI



Sumber: NRA TPPT dan PPSPM Tahun 2021

B. Kasus TPPT pada KUPVA Bukan Bank dan PTD Selain Bank

AJ (Putusan Nomor 817/Pid.Sus/2017/PN.Jkt.Tim)

AJ telah menganut pemahaman untuk melakukan jihad dengan kekerasan. Pada tahun 2014, AJ sering mengikuti perkembangan ISIS dari media sosial. Dalam mendukung perjuangan ISIS, AJ telah melakukan berbagai kegiatan, diantaranya dengan menjadi panitia yang memfasilitasi 15 (lima belas) orang keluarga berangkat ke Suriah. AJ juga aktif mengikuti kegiatan pelatihan militer.

Pada awal tahun 2015, AJ membuka rekening bank dengan dana awal sebesar Rp1.000.000,00 yang diberikan oleh ID. Lalu, AJ kembali mendapatkan tambahan dana sebesar Rp100.000.000,00. Kemudian, AJ mendapatkan tambahan dana sehingga jumlah dana pada rekeningnya mencapai Rp150.000.000,00.

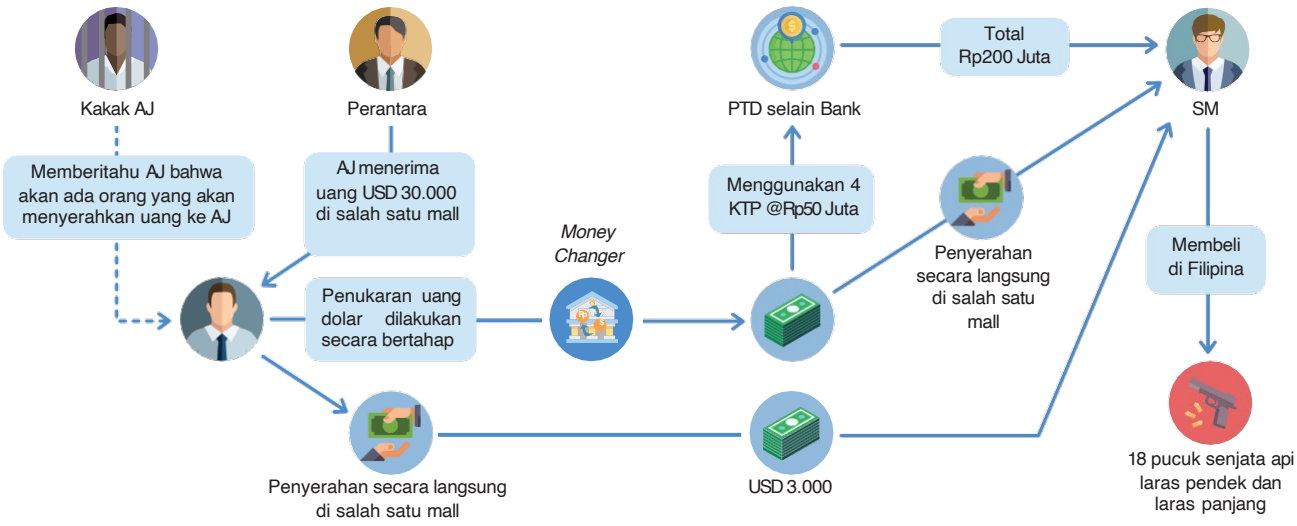
Pada September 2015, AJ memperoleh dana tambahan yang dikemas dalam bungkusan plastik berisi uang sebesar 30.000 USD dalam pecahan 100 USD. Kemudian, AJ menukarkan uang tersebut di beberapa *money changer*. Uang yang telah ditukarkan tersebut kemudian dikirimkan oleh AJ secara bertahap dengan rincian sebagai berikut:

1. 18.000 USD atau sekitar Rp200.000.000,00, dikirimkan melalui PTD Selain Bank melalui mitra bank dengan menggunakan KTP AS, KTP AKO, KTP M, dan KTP R, masing-masing Rp50.000.000,00.
2. 3.000 USD diserahkan secara tunai kepada SM.
3. Rp30.000.000,00 diserahkan secara tunai kepada SM.

Dana tersebut akan digunakan untuk pembelian senjata api sebanyak 18 (delapan belas) buah, yang terdiri dari senjata laras panjang dan pendek. Senjata api tersebut akan digunakan untuk melakukan aksi terorisme di Indonesia.

Skema Pendanaan Terorisme

Gambar 3.6. Skema Kasus AJ



Sumber: PPATK

Tipologi Pendanaan Terorisme

1. Pemindahan dana melalui penyedia jasa keuangan.
2. Pemindahan dana melalui pembawaan uang tunai lintas batas negara.
3. Penggunaan dana: Operasi terorisme domestik – pembelian senjata dan bahan peledak.

Red Flag

1. Transaksi dengan menggunakan identitas pihak lain.
2. Transaksi dalam jumlah relatif kecil, namun dilakukan secara bertahap.
3. Penukaran USD dalam jumlah besar.

3.3.3 Kasus PPSPM

Berdasarkan analisis yang dilakukan, selama tahun 2015-2020 belum terdapat kasus PPSPM yang melibatkan PJP Lembaga Selain Bank dan KUPVA Bukan Bank yang berada di bawah pengaturan dan pengawasan Bank Indonesia. Namun demikian, beberapa contoh kasus PPSPM yang diperoleh berdasarkan literatur, sebagai berikut:

Contoh Kasus I

Jaringan individu termasuk seorang ayah (Individu A), yang berbasis di Negara Y dan putranya (Individu B), yang berbasis di Negara Z, melakukan ekspor barang dan mesin asal Negara Z yang dapat digunakan untuk memproduksi senjata pemusnah massal atau *Weapon Mass Destruction* (WMD). Pada tahun 2008, Individu A dan salah satu perusahaan dijerat hukuman oleh pihak berwenang Negara Y sehubungan dengan pengiriman barang yang dibatasi ke Negara X. Jaringan ini terdiri dari setidaknya tiga perusahaan yang berbasis di Negara Y yang didirikan dan dikelola oleh Individu A. Pada bulan Januari 2009, Departemen Keuangan Negara Z menetapkan Individu A dan dua perusahaan yang terlibat sebagai tersangka, karena mendukung entitas X yang erat kaitannya dengan program WMD Negara X. Meskipun telah ditetapkan sebagai tersangka, Individu A tetap mengimpor alat mesin dari Negara Z melalui perusahaan di Negara Y yang tidak ditetapkan sebagai tersangka dengan bantuan Individu B. Pada pertengahan 2009, pihak berwenang Negara Z mengetahui bahwa Individu A akan bertemu dengan perwakilan entitas X di Negara D. Adapun keterlibatan entitas yang terindikasi terlibat program WMD dalam transaksi dan pembayaran ini disembunyikan, karena transaksi tersebut dilakukan melalui *wire transfer* dari rekening Bank Negara Y ke rekening milik Individu B di Negara Z. Demikian pula, transfer keuangan berikutnya dari Individu A dan Individu B menggunakan dua *wire transfer* dari rekening bank di Negara Y yang dikendalikan oleh Individu C, yang berusaha menyembunyikan keterlibatan Individu A yang telah terindikasi terlibat dalam program WMD dari sistem perbankan Negara Z. Individu C juga berhasil mendirikan perusahaan yang berbasis di Negara Z, untuk membantu mengembangkan bisnis dengan perusahaan Individu A.

Tipologi PPSPM

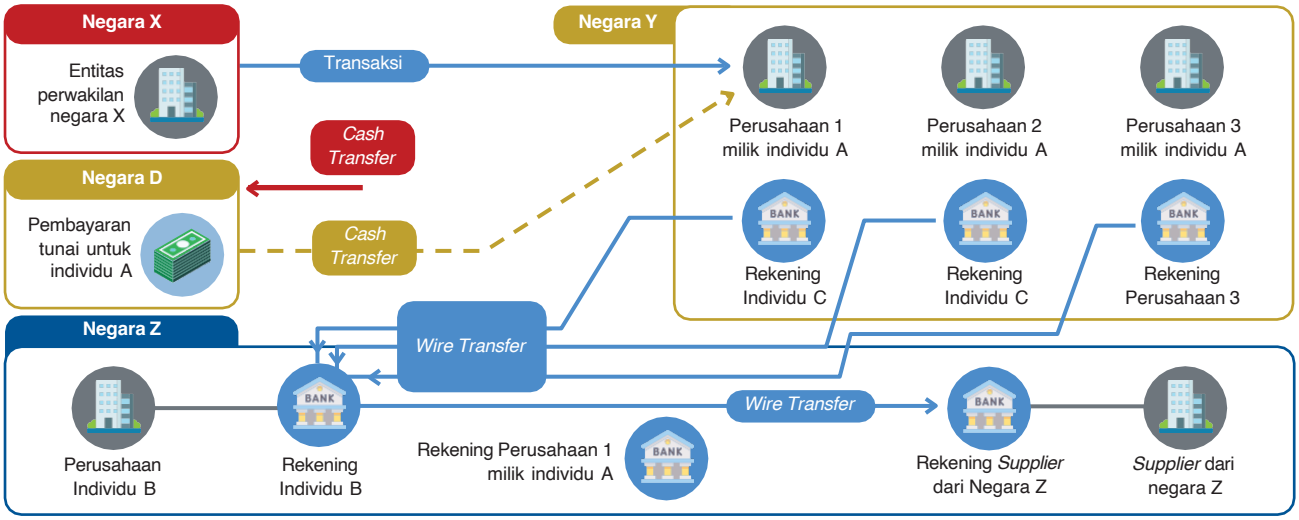
1. Transaksi ekspor-impor yang melibatkan barang-barang yang dikendalikan dalam rezim kontrol ekspor PPSPM.
2. Transaksi melibatkan entitas yang memiliki hubungan dengan negara yang rentan terhadap praktik PPSPM.
3. Penggunaan *front company* dalam transaksi.
4. Transaksi yang dilakukan antar perusahaan.
5. Transaksi menggunakan *wire transfer*.
6. Transaksi melibatkan orang atau entitas dari luar negeri yang ditujukan untuk menyamarkan aliran dana.

Red Flag

1. Melakukan ekspor barang dan mesin yang dapat digunakan untuk memproduksi WMD.
2. Adanya pertemuan antara pihak yang melakukan kegiatan ekspor barang untuk memproduksi WMD dengan entitas negara yang rentan proliferasi.
3. Pembayaran dilakukan melalui beberapa transaksi *wire transfer*, yang melibatkan berbagai pihak.

Skema PPSPM

Gambar 3.7. Skema Contoh Kasus I PPSPM



Sumber: Gibraltar FIU (2020)

Contoh Kasus II

Perusahaan X melakukan penyediaan dukungan untuk PPSPM. Perusahaan X diketahui menggunakan praktik penipuan, termasuk penciptaan dan penggunaan *Front Company* untuk menghindari sanksi dan terlibat dalam transaksi keuangan dengan bank di Negara A. Kementerian Keuangan menerima informasi tentang kemungkinan adanya *Front Company*. Berdasarkan informasi pemerintah, Kementerian Keuangan mulai mengembangkan pembuktian dan menetapkan *Front Company* Perusahaan X sebagai tersangka dalam penggunaan sistem keuangan Negara A untuk melakukan pembayaran yang mendukung aktivitas proliferasi. Informasi keuangan digunakan dalam pengembangan kasus dan dakwaan yang sesuai terhadap orang dan entitas yang terlibat. Misalnya, dalam dokumen pembukaan rekening untuk mendirikan salah satu *Front Company*, alamat dan nomor telepon yang tercantum sama dengan milik dari Perusahaan X.

Tipologi PPSPM

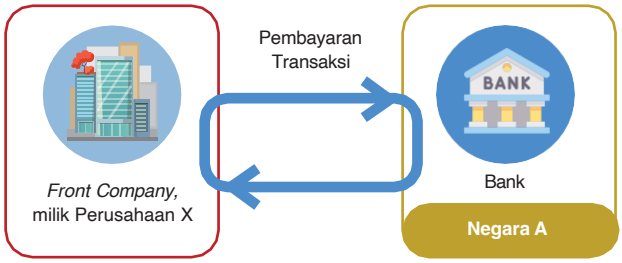
1. Penggunaan *front company* dalam transaksi.
2. Transaksi yang melibatkan barang-barang yang dikendalikan dalam rezim kontrol ekspor PPSPM.
3. Transaksi yang melibatkan seseorang yang memiliki hubungan dengan negara yang rentan dengan praktik PPSPM.
4. Penggunaa dokumen, alamat, dan nomor telepon yang sama dengan milik Perusahaan X untuk melakukan pembukaan rekening dan mendirikan *Front Company*.

Red Flag

1. Pembukaan rekening untuk pendirian *front company* yang menggunakan dokumen, alamat, dan nomor telepon yang sama dengan milik salah satu perusahaan pelaku.
2. Adanya keterlibatan dengan entitas yang rentan dengan aktivitas proliferasi.

Skema PPSPM

Gambar 3.8. Skema Contoh Kasus II PPSPM



Contoh Kasus III

Jaringan A merupakan jaringan yang memanfaatkan *Front Company* untuk menghindari sanksi dalam mendukung program proliferasi dan rudal Negara X. Pada tahun 2010 dan 2015, Individu A dan Individu B, beserta rekannya menjalankan jaringan yang berkonspirasi untuk melakukan transaksi keuangan internasional atas nama dan untuk kepentingan Negara X. Para konspirator mengoperasikan jaringan perusahaan internasional, termasuk perusahaan perdagangan dan bisnis keuangan yang berlokasi di Negara X, Negara Y, dan Negara Z, serta tempat lain untuk menyembunyikan transaksi yang dilakukan atas nama entitas Negara X. Adapun konspirator lainnya yaitu termasuk Menteri Ekonomi Negara Y dan tiga orang eksekutif dari Bank D milik Pemerintah Y. Bank tersebut digunakan untuk memfasilitasi transfer mata uang dan emas jaringan A ke atau dari entitas Negara X yang terkena sanksi, sementara juga menyembunyikan peran bank dalam menghindarkan sanksi Negara C. Aktivitas ini meliputi transfer hasil minyak Negara X untuk menukar *front company* yang dikendalikan oleh Individu A dengan *front company* yang memungkinkan pembelian emas untuk ekspor dari Negara Y. Setelah diekspor dari Negara Y, emas dapat dikonversi menjadi uang tunai atau mata uang dan dikirim ke Negara X atau digunakan untuk melakukan transfer keuangan internasional atas nama orang dan entitas Negara X. Menteri Negara Y, diduga mengarahkan para bankir Negara Y untuk terlibat dalam beberapa jenis transaksi untuk melindungi skema ini. Pada Maret 2016, Individu A ditangkap. Individu A bersaksi tentang rincian operasi ilegal, termasuk penggunaan dokumentasi palsu, *Front Company*, dan langkah-langkah penipuan lainnya untuk mengakses Negara C atas nama Pemerintah dan entitas Negara X. Salah satu tipologi yang digunakan oleh rekan konspirator adalah membuat dan menggunakan dokumen palsu untuk menyamarkan transaksi ilegal. Hal ini menyebabkan bank-bank Negara C secara tanpa sadar, memproses transaksi keuangan internasional tersebut.

Tipologi PPSPM

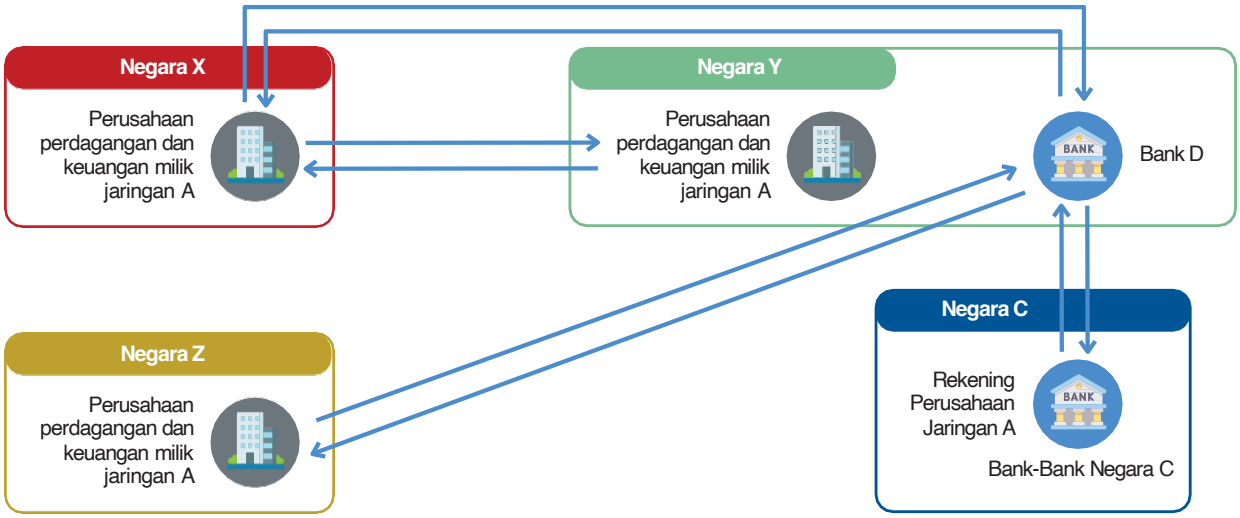
1. Penggunaan *Front Company* dalam transaksi.
2. Transaksi yang melibatkan barang-barang yang dikendalikan dalam rezim kontrol ekspor PPSPM.
3. Transaksi yang melibatkan seseorang yang memiliki hubungan dengan negara yang rentan dengan praktik PPSPM.
4. Transaksi menggunakan logam mulia.
5. Keterlibatan perusahaan perdagangan kecil atau perusahaan perantara yang melakukan kegiatan bisnis tidak sesuai dengan kegiatan usahanya.
6. Perusahaan yang melakukan pengiriman uang.
7. Transaksi menggunakan dokumen fiktif atau tidak valid.

Red Flag

1. Adanya keterlibatan dengan entitas atau negara yang rentan dengan aktivitas proliferasi.
2. Transaksi internasional yang dilakukan untuk dan atas nama entitas atau negara yang rentan dengan aktivitas proliferasi.
3. Pendirian dan penggunaan perusahaan perdagangan dan bisnis keuangan yang berlokasi di berbagai negara.
4. Penggunaan logam mulia, seperti emas untuk bertransaksi dengan entitas atau negara yang rentan dengan aktivitas proliferasi.
5. Penggunaan dokumen palsu dalam melakukan transaksi.

Skema PPSPM

Gambar 3.9. Skema Contoh Kasus III PPSPM



Contoh Kasus IV

Pada tahun 2013, otoritas A menahan sebuah Kapal Negara X yang melakukan perjalanan dari Negara Y ke Negara X dan transit di wilayah A. Otoritas tersebut menemukan pengiriman senjata dan bahan terkait proliferasi yang disembunyikan di bawah kargo. Adapun biaya perjalanan pengiriman tersebut dibayar oleh Perusahaan B yang berbasis di Negara D. Perusahaan B memiliki hubungan bisnis dengan perusahaan pengiriman Negara X sejak tahun 1980-an. Perusahaan B merupakan agen pengiriman dan importir/eksportir grosir umum. Perusahaan tersebut merupakan salah satu dari tiga perusahaan yang dijalankan oleh keluarga yang memiliki alamat bisnis, karyawan, dan akun email yang sama untuk komunikasi dengan entitas Negara X. Ketiga perusahaan juga memiliki rekening yang sama di Bank Negara D, atas nama Perusahaan B. Selama 3 (tiga) tahun, sekitar 605 (enam ratus lima) pengiriman uang terjadi dengan total lebih dari USD 40 juta, seluruhnya berkaitan dengan kapal Negara X. Perusahaan B juga ditemukan secara aktif melakukan kegiatan pengiriman uang, meskipun perusahaan tersebut tidak memiliki izin untuk melakukannya. Perusahaan B berusaha untuk menyembunyikan keterlibatannya dengan perusahaan Negara X dengan menghapus nama-nama kapal dan rincian identifikasi lainnya dari formulir pengiriman uang dan korespondensi *email*. Pembayaran dari akun Perusahaan B terjadi tanpa adanya faktur ataupun informasi lainnya. Perusahaan B akhirnya dihukum karena melakukan pembiayaan proliferasi sebesar USD 72.016,76 yang dikirimkan melalui transfer dari rekening Bank Negara D ke rekening perusahaan pengiriman Negara A.

Tipologi PPSPM

1. Transaksi melibatkan barang-barang yang dikendalikan dalam rezim kontrol ekspor PPSPM.
2. Transaksi melibatkan negara yang rentan terhadap aktivitas proliferasi.
3. Transaksi yang melibatkan seseorang atau entitas yang memiliki hubungan dengan negara yang rentan dengan praktik PPSPM.
4. Pembayaran transaksi dilakukan oleh entitas lain.
5. Penggunaan *Front Company*.
6. Perusahaan dijalankan oleh keluarga yang memiliki alamat bisnis, karyawan, dan akun *email* yang sama.
7. Perusahaan menggunakan rekening yang sama untuk bertransaksi.

8. Perusahaan yang melakukan transaksi pengiriman uang secara ilegal.

9. Transaksi menggunakan *wire transfer*.

10. Transaksi tanpa disertai dengan dokumen pendukung, seperti faktur atau rincian informasi lainnya.

Red Flag

1. Adanya pengiriman senjata dan bahan terkait proliferasi yang memiliki tujuan ke negara yang rentan aktivitas proliferasi.

2. Pembayaran biaya pengiriman dilakukan oleh entitas lain yang memiliki hubungan dengan entitas atau negara yang rentan aktivitas proliferasi, serta dilakukan dengan *wire transfer.*

3. Adanya keterlibatan perusahaan yang bergerak dalam usaha pengiriman dan ekspor-impor.

4. Perusahaan dijalankan oleh keluarga yang memiliki alamat bisnis, karyawan, dan akun *email* yang sama, untuk berkomunikasi dengan entitas atau negara yang rentan aktivitas proliferasi.

5. Adanya aktivitas bisnis pengiriman uang ilegal.

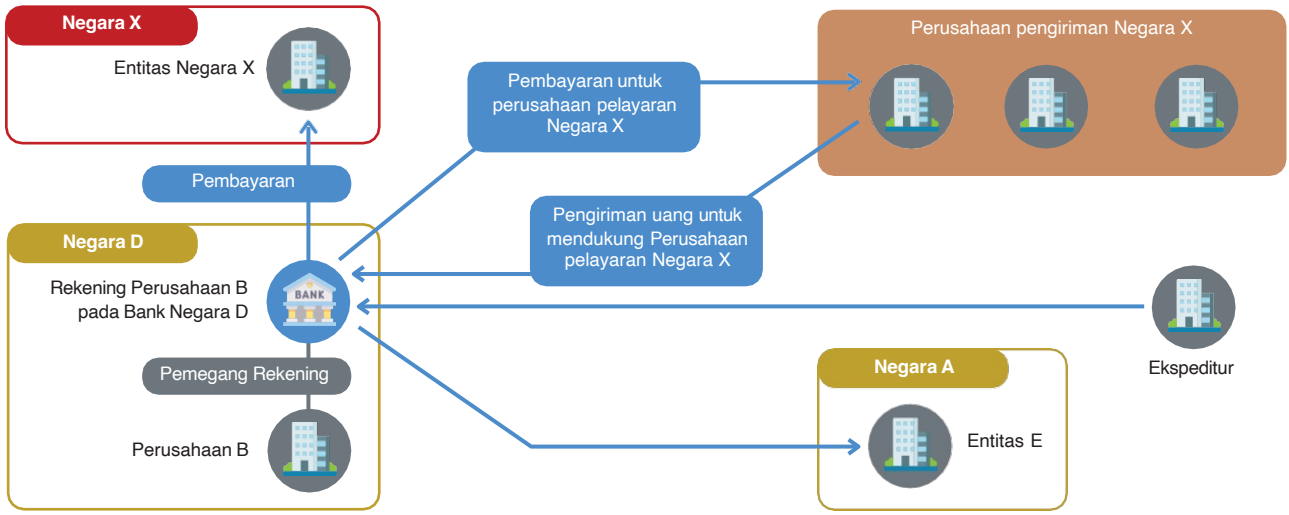
6. Adanya penghapusan nama-nama kapal dan rincian identifikasi lainnya dari formulir pengiriman.

Contoh Kasus V

Suatu entitas Negara X melalui salah satu jaringan PPSPM mencoba untuk menggunakan sistem keuangan Negara Y dan melibatkan jaringan di Negara X, Negara L, Negara Y, yang diduga bekerja untuk mengekspor peralatan laboratorium kimia terbatas secara ilegal ke Negara X. Kasus ini melibatkan dua individu keturunan Negara X (Individu A dan B) dan seorang pria asal Negara Y (Individu C) yang mengoperasikan bisnis ekspor yang berbasis di Negara Y. Jaringan ini memfasilitasi penerimaan peralatan laboratorium kimia atas nama pelanggan dari Negara X dan mengekspor barang-barang ini ke Negara X melalui negara- negara pihak ketiga seperti Negara A, Negara B, dan Negara L. Dalam mencapai hal tersebut, rekan konspirator membuat faktur palsu dan memberikan label yang salah pada barang yang dibeli di Negara Y, serta menggunakan informasi palsu mengenai identitas pembeli dan lokasi geografis. Pembiayaan skema ini terutama dilakukan melalui serangkaian *wire transfer* internasional yang berasal dari rekening bank

Skema PPSPM

Gambar 3.10. Skema Contoh Kasus IV PPSPM



Sumber: Gibraltar FIU (2020)

Negara D milik anggota jaringan tersebut, ke fasilitator di Negara Y. Seringkali transaksi *wire transfer* tersebut menggunakan informasi yang tidak jelas. Transfer ini juga bernilai relatif kecil, mulai dari USD 500 hingga USD 18.000.

Tipologi PPSPM

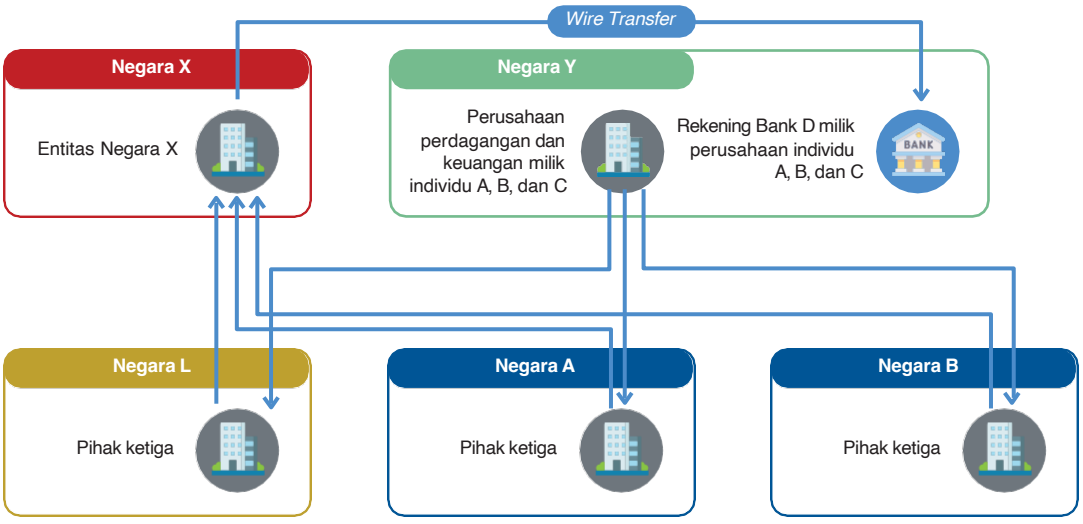
1. Transaksi melibatkan barang-barang yang dikendalikan dalam rezim kontrol ekspor PPSPM.
2. Transaksi melibatkan negara yang rentan terhadap aktivitas proliferasi.
3. Transaksi yang melibatkan seseorang atau entitas yang memiliki hubungan dengan negara yang rentan dengan praktik PPSPM.
4. Transaksi yang melibatkan seseorang atau entitas dari negara yang rentan dengan praktik PPSPM.
5. Transaksi menggunakan dokumen fiktif atau tidak valid.
6. Transaksi menggunakan identitas palsu.
7. Pengguna jasa memberikan informasi yang tidak valid, terutama yang berkaitan dengan barang atau jasa yang diekspor.
8. Transaksi menggunakan informasi fiktif terkait lokasi pengiriman.
9. Transaksi menggunakan *wire transfer*.

Red Flag

1. Adanya keterlibatan entitas atau negara yang rentan dengan aktivitas proliferasi.
2. Kegiatan ekspor peralatan kimia secara ilegal ke negara yang rentan aktivitas proliferasi.
3. Transaksi yang melibatkan orang atau entitas yang memiliki hubungan atau berasal dari negara yang rentan aktivitas proliferasi.
4. Penggunaan dokumen dan informasi fiktif terkait barang, identitas pembeli, dan lokasi geografis.
5. Transaksi *wire transfer* dengan informasi yang tidak jelas.

Skema PPSPM

Gambar 3.11. Skema Contoh Kasus V PPSPM



Contoh Kasus VI

MI, dan kedua putranya (K dan IK), terlibat dalam skema pembelian barang-barang yang dikendalikan oleh peraturan administrasi ekspor dan mengekspor barang-barang tersebut secara ilegal ke Negara X, yang melanggar peraturan administrasi ekspor. Melalui serangkaian *Front Company* yang berlokasi di Negara X dan Negara Y, ketiga orang tersebut menerima perintah dari sebuah Perusahaan Negara X untuk mendapatkan bahan dan peralatan yang berkaitan dengan senjata nuklir dan program rudal balistik Negara X. Dalam mendapatkan bahan dan peralatan tersebut, jaringan tersebut memperolehnya melalui produsen dari Negara Y. Namun, ketika produsen Negara Y menanyakan tentang penggunaan akhir untuk suatu produk, jaringan tersebut menginformasikan bahwa produk tersebut akan tetap berada di Negara Y atau menunjukkan sertifikasi yang menyatakan bahwa produk tersebut tidak akan diekspor. Setelah produk dibeli, produk dikirim oleh produsen ke pihak di Negara Y. Produk-produk itu kemudian dikirim ke *front company* yang bertindak atas nama entitas Negara X, yang bertanggung jawab untuk memastikan bahwa barang-barang itu diserahkan kepada Komisi di Negara X. Beberapa bahan yang diperoleh disampaikan kepada program pengembangan rudal Negara X. Dalam kasus ini, MI dan kedua putranya tidak pernah memperoleh lisensi untuk mengekspor barang. Mereka menerima hasil penjualan barang-barang tersebut melalui *wire transfer* dari entitas yang berbasis di Negara X dan Negara Z ke rekening bank Negara Y. Pada 1 Juni 2017, IK dijatuhi hukuman atas tindakan pelanggaran hukuman yang dilakukan karena mengekspor peralatan militer secara ilegal.

Tipologi PPSPM

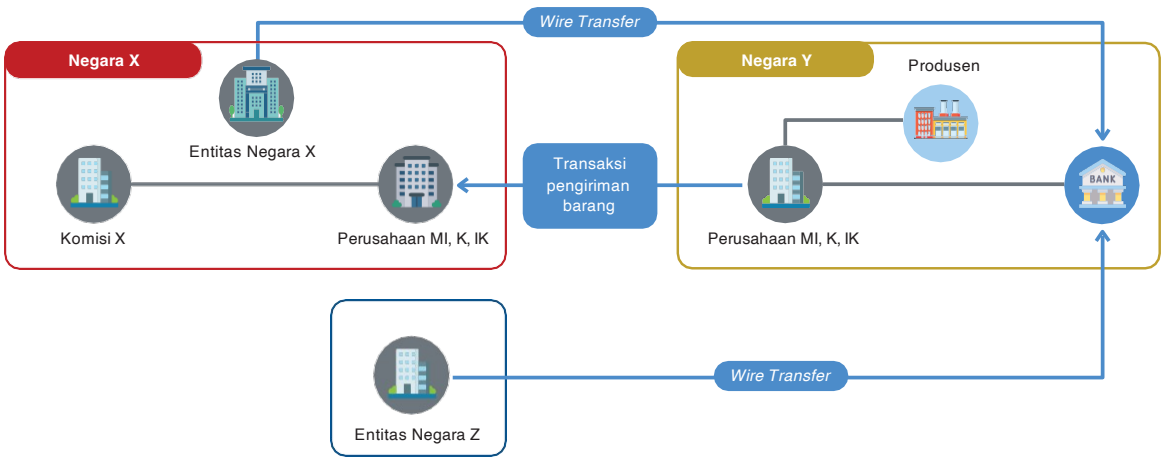
1. Transaksi melibatkan barang-barang yang dikendalikan dalam rezim kontrol ekspor PPSPM.
2. Transaksi melibatkan negara yang rentan terhadap aktivitas proliferasi.
3. Transaksi yang melibatkan seseorang atau entitas yang memiliki hubungan dengan negara yang rentan dengan praktik PPSPM.
4. Transaksi yang melibatkan seseorang atau entitas dari negara yang rentan dengan praktik PPSPM.
5. Penggunaan *Front Company* dalam transaksi.
6. Transaksi menggunakan *wire transfer*.

Red Flag

1. Pembelian barang-barang yang terkait dengan rezim ekspor-impor WMD.
2. Transaksi yang melibatkan serangkaiann *front company* dari berbagai negara.
3. Transaksi yang melibatkan entitas atau negara yang rentan aktivitas proliferasi.
4. Pembayaran transaksi melalui *wire transfer* dari entitas yang berada di negara yang rentan aktivitas proliferasi.

Skema PPSPM

Gambar 3.12. Skema Contoh Kasus VI PPSPM



Contoh Kasus VII

Negara X menetapkan Entitas B dan jaringannya, untuk menyediakan dan memberikan dukungan finansial, material, teknologi untuk mendukung Negara X. Entitas B adalah pemasok elektronik yang berbasis di Negara Y dan beroperasi di Negara X, Negara M, Negara C, dan Negara P, serta menjadi produsen barang-barang yang digunakan dalam produksi senjata pemusnah massal untuk Negara X. Entitas B menggunakan berbagai cabang perusahaan untuk melakukan kegiatannya. Pada hari yang sama, Entitas X menunjuk Individu A dan Individu B yang berasal dari Negara Y yang tinggal di salah satu kota di Negara Z untuk mengekspor barang dari Negara Z. Individu A dan Individu B ini mengoperasikan bisnis ekspor dari kediaman mereka. Pasangan itu menggunakan bisnis mereka untuk mendapatkan barang, termasuk elektronik, peralatan komputer, dan sakelar listrik, dari Perusahaan Negara Z dan mengekspor barang- barang itu keluar dari Negara Z ke pembeli di Negara Y dan Negara X, termasuk Entitas B. Pada tahun 2007, Entitas B dan pendirinya (MK dan AK), ditambahkan ke Daftar Pengawasan Departemen Perdagangan karena Pemerintah Negara Z telah menetapkan bahwa Entitas B terlibat dalam kegiatan yang berkaitan dengan PPSPM yang digunakan untuk melawan pasukan Negara Z dan Koalisi di Negara I dan Negara J. Pada tahun 2013, Individu A dan Individu B mulai melakukan bisnis dengan MK dan memasok barang-barang asal Negara Z ke Entitas B. Individu A dan Individu B juga mengetahui bahwa MK mengoperasikan bisnis di Negara X dan menyediakan layanan perantara.

Tipologi PPSPM

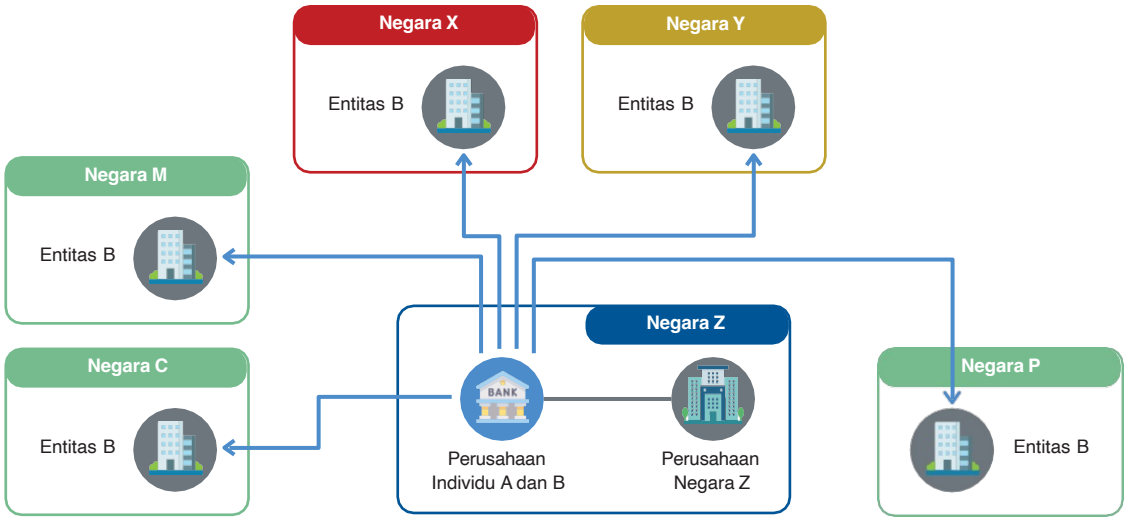
1. Transaksi melibatkan barang-barang yang dikendalikan dalam rezim kontrol ekspor PPSPM.
2. Transaksi melibatkan negara yang rentan terhadap aktivitas proliferasi.
3. Transaksi yang melibatkan seseorang atau entitas yang memiliki hubungan dengan negara yang rentan dengan praktik PPSPM.
4. Transaksi melibatkan perusahaan ekspor.

Red Flag

1. Adanya keterlibatan atau hubungan dengan entitas atau negara yang rentan dengan aktivitas proliferasi.
2. Penggunaan bisnis ekpor-impor.
3. Transaksi yang melibatkan barang-barang yang terkait WMD.

Skema PPSPM

Gambar 3.13. Skema Contoh Kasus VII PPSPM



BAGIAN 4

KESIMPULAN & REKOMENDASI

4.1 Kesimpulan

Berdasarkan hasil analisis tipologi kasus TPPU, TPPT, PPSPM pada PJP Lembaga Selain Bank dan KUPVA Bukan Bank, maka dapat disimpulkan beberapa hal diantaranya:

1. Berdasarkan data salinan putusan pengadilan tahun 2015-2020, terdapat 29 (dua puluh sembilan) kasus yang berkaitan dengan TPPU dan TPPT. Dari total putusan tersebut, sebanyak 24 (dua puluh empat) putusan merupakan perkara TPPU, sedangkan 5 (lima) putusan merupakan perkara TPPT. Pada data putusan pengadilan tahun 2015-2020 tidak ditemukan kasus yang berkaitan dengan PPSPM. Adapun dari putusan tersebut diperoleh beberapa informasi sebagai berikut:

    a. Profil pekerjaan pelaku yang dominan dari kasus TPPU dan TPPT selama tahun 2015- 2020 yaitu:

        1. Pada perkara TPPU, profil pekerjaan pelaku yang dominan adalah wiraswasta yaitu sebanyak 16 (enam belas) orang pelaku. Sementara itu, profil pekerjaan lainnya adalah pegawai swasta, PNS, pejabat pemerintahan, ibu rumah tangga, pegawai *money changer*, pengajar, dan lainnya.

        2. Pada perkara TPPT, terdapat pelaku yang profil pekerjaannya adalah wiraswasta. Selain itu, terdapat pelaku yang tidak bekerja, serta yang tidak dapat diidentifikasi profil pekerjaannya.

    b. Profil badan usaha yang dominan dari kasus TPPU dan TPPT selama tahun 2015-2020 yaitu:

        1. Pada perkara TPPU, profil badan usaha yang terlibat didominasi oleh Perusahaan Non UMKM berbentuk PT, yaitu sebanyak 11 (sebelas) kasus. Profil badan usaha lainnya adalah CV. Selain itu, terdapat kasus yang tidak dapat diidentifikasi profil badan usahanya.

        2. Pada perkara TPPT, tidak dapat diidentifikasi profil badan usaha yang terlibat.

    c. Berdasarkan karakteristik sebaran wilayah dari kasus TPPU dan TPPT selama tahun 2015-2020 yaitu:

        1. Pada perkara TPPU, sebagian besar perkara berada di DKI Jakarta, yaitu sebanyak 20 (dua puluh) kasus. Adapun sebaran wilayah lainnya yaitu Kalimantan Barat, Banten, dan Lampung.

        2. Pada perkara TPPT, sebagian besar perkara berada di DKI Jakarta, yaitu sebanyak 3 (tiga) kasus. Meskipun demikian, terdapat juga kasus yang tidak dapat diidentifikasi wilayahnya.

    d. Produk dan layanan yang digunakan dalam kasus TPPU dan TPPT selama tahun 2015- 2020 yaitu:

        1. Pada perkara TPPU, produk dan layanan yang dominan digunakan pada KUPVA Bukan Bank adalah produk UKA USD, diikuti SGD, dan EUR. Sementara itu, mekanisme jual beli UKA yang dominan digunakan adalah Transfer Bank. Sedangkan pada PTD Selain Bank, produk dan layanan yang dominan digunakan yaitu *Account to Account (incoming)*, dan *Cash to Account (outgoing)*.

        2. Pada perkara TPPT, produk dan layanan yang dominan digunakan pada KUPVA Bukan Bank adalah produk UKA USD.

Sementara itu mekanisme jual beli UKA tidak dapat diidentifikasi. Sedangkan pada PTD Selain Bank, produk dan layanan yang dominan digunakan yaitu *Cash to Account (Outgoing),* diikuti *Account to Account (Outgoing).*

e. *Delivery channel* yang digunakan dalam kasus TPPU dan TPPT selama tahun 2015-2020 yaitu:

1. Pada perkara TPPU, *delivery channel* yang dominan digunakan adalah Kantor KUPVA Bukan Bank, yaitu sebanyak 22 (dua puluh dua) kasus. Untuk *delivery channel* lainnya yang digunakan adalah Kantor PTD Bukan Bank.

2. Pada perkara TPPT, *delivery channel* yang dominan digunakan adalah Kantor PTD Bukan Bank, yaitu sebanyak 4 (empat) kasus. Untuk *delivery channel* lainnya yang digunakan adalah Kantor KUPVA Bukan Bank.

2. Berdasarkan data hasil survei yang dilakukan pada penyelenggara KUPVA Bukan Bank, PTD Selain Bank, Penyelenggara UE dan DE Selain Bank, serta Penyelenggara APMK Selain Bank, didapatkan bahwa:

a. Tipologi TPPU dan TPPT pada penyelenggara KUPVA Bukan Bank, antara lain:

1. Terdapat 3 (tiga) tipologi TPPU yang memiliki risiko tertinggi pada KUPVA Bukan Bank yaitu penggunaan identitas palsu, *mingling*, serta *trade-based money laundering* dan *transfer pricing*.

2. Terdapat 3 (tiga) tipologi TPPT yang memiliki risiko tertinggi pada KUPVA Bukan Bank yaitu Penggunaan Dana: Operasi Terorisme Domestik—Pembelian Senjata dan Bahan Peledak, Penggunaan Dana: Operasi Terorisme Domestik - Dokumen Identitas Palsu, Penggunaan Dana: Operasi Terorisme Domestik - Perjalanan dari dan ke lokasi aksi terorisme.

b. Tipologi TPPU dan TPPT pada PTD Selain Bank, antara lain:

1. Terdapat 3 (tiga) tipologi TPPU yang memiliki risiko tertinggi pada PTD Selain Bank yaitu *smurfing*, aktivitas perjudian *online*, dan *structuring*.

2. Terdapat 3 (tiga) tipologi TPPT yang memiliki risiko tertinggi pada PTD Selain Bank yaitu Pengumpulan Dana - Ilegal: Hasil Kejahatan Kriminal Lainnya, Penggunaan Dana: Operasi Terorisme Domestik - Dokumen Identitas Palsu, Penggunaan Dana: Operasi Terorisme Domestik - Perjalanan dari dan ke lokasi aksi terorisme.

c. Tipologi TPPU dan TPPT pada penyelenggara UE dan DE Selain Bank, antara lain:

1. Terdapat 3 (tiga) tipologi TPPU yang memiliki risiko tertinggi pada penyelenggara UE dan DE Selain Bank yaitu penggunaan identitas palsu, *smurfing*, dan aktivitas perjudian *online*.

2. Terdapat 3 (tiga) tipologi TPPT yang memiliki risiko tertinggi pada penyelenggara UE dan DE Selain Bank yaitu Pengumpulan Dana - Ilegal: Penculikan dengan Tebusan, Pengumpulan Dana - Ilegal: Hasil Kejahatan Kriminal Lainnya, dan Penggunaan Dana: Operasi Terorisme Domestik - Perjalanan dari dan ke lokasi aksi terorisme.

d. Tipologi TPPU dan TPPT pada penyelenggara APMK Selain Bank, antara lain:

   1. Terdapat 3 (tiga) tipologi TPPU yang memiliki risiko tertinggi pada penyelenggara APMK Selain Bank yaitu penggunaan identitas palsu, pemanfaatan internet enkripsi, akses terhadap identitas, perbankan internasional, serta pemanfaatan Kartu Kredit, Cek, Surat Perjanjian Hutang.

   2. Terdapat 3 (tiga) tipologi TPPT yang memiliki risiko tertinggi pada penyelenggara APMK Selain Bank yaitu Pengumpulan Dana - Legal: Sponsor Pribadi *(Terrorist Financier/ Fundraiser)*, Pengumpulan Dana - Legal: Penyimpangan Pengumpulan Donasi Melalui Ormas, Pengumpulan Dana - Legal: Pendanaan *Crowdfunding*.

3. Berdasarkan data hasil survei yang dilakukan pada penyelenggara KUPVA Bukan Bank, PTD Selain Bank, Penyelenggara UE dan DE Selain Bank, serta Penyelenggara APMK Selain Bank, tidak ditemukan adanya modus/tipologi yang berkaitan dengan PPSPM. Meskipun demikian, berdasarkan hasil penelitian dari berbagai sumber literatur ditemukan beberapa tipologi yang berkaitan dengan PPSPM yaitu:

   1. Transaksi ekspor-impor yang melibatkan barang-barang yang dikendalikan dalam rezim kontrol ekspor PPSPM;
   2. Transaksi melibatkan entitas yang memiliki hubungan dengan negara yang rentan terhadap praktik PPSPM;
   3. Penggunaan *front company* dalam transaksi;
   4. Transaksi yang dilakukan antar perusahaan;
   5. Transaksi menggunakan *wire transfer*;
   6. Transaksi melibatkan orang atau entitas dari luar negeri yang ditujukan untuk menyamarkan aliran dana;
   7. Penggunaan dokumen, alamat, dan nomor telepon yang sama dengan milik suatu perusahaan untuk melakukan pembukaan rekening dan mendirikan *Front Company*;
   8. Transaksi menggunakan logam mulia;
   9. Keterlibatan perusahaan perdagangan kecil atau perusahaan perantara yang melakukan kegiatan bisnis tidak sesuai dengan kegiatan usahanya;
   10. Perusahaan yang melakukan pengiriman uang;
   11. Transaksi menggunakan dokumen fiktif atau tidak valid;
   12. Transaksi melibatkan negara yang rentan terhadap aktivitas proliferasi;
   13. Pembayaran transaksi dilakukan oleh entitas lain;
   14. Perusahaan dijalankan oleh keluarga yang memiliki alamat bisnis, dan akun *email* yang sama;
   15. Perusahaan menggunakan rekening yang sama untuk bertransaksi;
   16. Transaksi tanpa disertai dengan dokumen pendukung, seperti faktur atau rincian lainnya;
   17. Transaksi yang melibatkan individu atau entitas dari negara yang rentan dengan praktik PPSPM;
   18. Transaksi menggunakan identitas palsu;
   19. Pengguna jasa memberikan informasi yang tidak valid, terutama yang berkaitan dengan barang atau jasa yang di ekspor;
   20. Transaksi menggunakan informasi fiktif terkait lokasi pengiriman;
   21. Transaksi melibatkan perusahaan ekspor.

4.2 Rekomendasi

Berdasarkan hasil analisis tipologi kasus TPPU, TPPT, PPSPM pada PJP Lembaga Selain Bank dan KUPVA Bukan Bank, terdapat beberapa rekomendasi yang ditujukan bagi Bank Indonesia maupun *stakeholder* eksternal, antara lain:

I. Rekomendasi kepada Bank Indonesia

1. Melakukan diseminasi hasil analisis tipologi TPPU, TPPT, PPSPM kepada pegawai sektor sistem pembayaran khususnya yang menangani pengaturan, perizinan, dan pengawasan dalam rangka penguatan implementasi RBA APU PPT.
2. Melakukan *capacity building* secara reguler khususnya kepada pegawai yang menangani pengawasan untuk meningkatkan *awareness* terkait APU PPT serta meningkatkan kinerja pengawasan dalam upaya pencegahan dan pemberantasan praktik TPPU, TPPT, dan PPSPM.
3. Mendiseminasikan hasil analisis tipologi TPPU, TPPT, PPSPM kepada seluruh penyelenggara dalam rangka peningkatan *awareness* dan mitigasi potensi risiko TPPU, TPPT, dan PPSPM pada sektor sistem pembayaran.
4. Melakukan penguatan mitigasi risiko TPPU, TPPT, dan PPSPM berdasarkan analisis tipologi yang telah dilakukan. Penguatan mitigasi baik oleh pengawas maupun PJP Lembaga Selain Bank dan KUPVA Bukan Bank melalui implementasi APU PPT berbasis risiko *(Risk Based Approach*-RBA*)*.
5. Memperkuat koordinasi dan kerjasama kelembagaan dengan otoritas dan instansi lain baik dalam negeri maupun luar negeri terutama terkait:
   a. Penyusunan *watchlist* bersama antara K/L dan penyelenggara dalam rangka mitigasi TPPU, TPPT, PPSPM;
   b. Penyusunan dan *sharing* tipologi TPPU, TPPT, PPSPM antara K/L dan penyelenggara sebagai acuan penerapan *red flag* pada transaksi pengguna jasa;
   c. Peningkatan upaya penertiban KUPVA Tidak Berizin dan PJP Ilegal;
   d. Optimalisasi *Public Private Partnership* (PPP) dalam rangka penyusunan *watchlist,* tipologi, serta peningkatan upaya penertiban KUPVA Tidak Berizin dan PJP Ilegal.
6. Melakukan kampanye akan pentingnya APU PPT kepada masyarakat luas, serta dampak negatif TPPU, TPPT, PPSPM terhadap perekonomian Indonesia.

II. Rekomendasi kepada PJP Lembaga Selain Bank dan KUPVA Bukan Bank di bawah Pengawasan Bank Indonesia

1. Mengadopsi hasil analisis tipologi TPPU, TPPT, dan PPSPM dalam rangka peningkatan mitigasi risiko TPPU, TPPT, dan PPSPM dan penguatan implementasi RBA APU PPT pada operasional perusahaan.
2. Melakukan diseminasi hasil NRA dan SRA kepada seluruh pegawai dalam rangka peningkatan *awareness* atas potensi risiko TPPU, TPPT, dan PPSPM.
3. Melakukan kampanye akan pentingnya APU PPT kepada masyarakat luas, serta memberikan edukasi kepada pengguna jasa akan pentingnya implementasi APU PPT khususnya pada proses CDD.
4. Penguatan implementasi RBA APU PPT melalui penerapan *Regulatory Technology* (*Regtech*) baik pada proses identifikasi dan verifikasi, maupun *on going due diligence* terhadap profil dan transaksi yang dilakukan pengguna jasa.

Daftar Pustaka

APG. 2020. APG *Yearly Typologies Report: Methods and Trends of Money Laundering and Terrorism Financing*. http://www.apgml.org/methods-and-trends/documents/default.aspx?s=date&c=2f18e690-1838-4310-b16a-8112ffa857b1.

APG. 2021. APG Yearly Typologies Report: Methods and Trends of Money Laundering and Terrorism Financing. http://www.apgml.org/methods-and-trends/page.aspx?p=8d052c1c-b9b8-45e5-9380-29d5aa129f45.

Bank Indonesia. 2019. Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang dan Tindak Pidana Pendanaan Terorisme Sektor PJSP Selain Bank dan KUPVA Bukan Bank. https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/anti-pencucian-uang-dan-pencegahan-pendanaan-terrorisme/Documents/ SRA_id.pdf.

Brewer, Jonathan. 2018. *The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation*. Centre for a New American Security. https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation#:~:text=The%20financiers%20of%20proliferation%20of%20nuclear%20and%20other,or%20treaties%20such%20as%20the%20Nuclear%20Nonproliferation%20Treaty.

FATF. 2007. *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures*. https://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf.

FATF. 2010. FATF *Report*: *Money Laundering through Money Remittance and Currency Exchange Providers*. https://www.fatf-gafi.org/media/fatf/ML%20%through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf.

FATF. 2018. *Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction*. https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf.

FATF. 2021. *FATF Report: Money Laundering from Environmental Crime*. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-from-Environmental-Crime.pdf

FATF. 2021. *Guidance on Proliferation Financing Risk Assessment and Mitigation*. https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.

Gibraltar. 2020. *Gibraltar Financial Intelligence Unit and Gibraltar Financial Services Commission, Counter Proliferation Financing: Guidance Notes*. https://www.gfiu.gov.gi/uploads/docs/X86Ru_CPF_Guidance_Notes_v1.1.pdf.

PPATK. 2019. Surat Edaran No. 8 Tahun 2019: Indikator Transaksi Keuangan Mencurigakan terkait Tindak Pidana Narkotika. https://jdih.ppatk.go.id/produk-hukum/detail/9/surat-edaran-kepala-ppatk-nomor-08-tahun-2019-tentang-indikator-transaksi-keuangan-mencurigakan-terkait-tindak-pidana-narkotika.

PPATK. 2019. Tipologi Pencucian Uang Berdasarkan Putusan Pengadilan Tahun 2018. https://www.ppatk.go.id//backend/assets/images/publikasi/1581670316_.pdf.

PPATK. 2020. Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang Hasil Tindak Pidana Kehutanan. https://www.ppatk.go.id/publikasi/read/114/penilaian-risiko-sektoral-tindak-pidana-pencucian-uang-hasil-tindak-pidana-kehutanan.html.

PPATK. 2020. Tipologi Pencucian Uang Berdasarkan Putusan Pengadilan Tahun 2019. https://www.ppatk.go.id//backend/assets/images/publikasi/1615872606_.pdf.

PPATK. 2021. Penilaian Risiko Pidana Pencucian Uang Berbasis Perdagangan.

PPATK. 2021. Surat Edaran No. 2 Tahun 2021: Indikator Transaksi Keuangan Mencurigakan terkait Tindak Pidana di Bidang Perpajakan. https://jdih.ppatk.go.id/produk-hukum/detail/132/surat-edaran-kepala-ppatk-nomor-02-tahun-2021-tentang-indikator-transaksi-keuangan-mencurigakan-terkait-tindak-pidana-di-bidang perpajakan.

PPATK. 2022. Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang Pada Tindak Pidana Penipuan Siber. https://www.ppatk.go.id/publikasi/read/165/penilaian-risiko-sektoral-tindak-pidana-pencucian-uang-pada-tindak-pidana-penipuan-siber-tahun-2022.html.

PPATK. 2022. Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang Hasil Tindak Pidana Korupsi. https://www.ppatk.go.id/publikasi/read/164/penilaian-risiko-sektoral-tindak-pidana-pencucian-uang-hasil-tindak-pidana-korupsi-tahun-2022.html#.

United Nations Office on Drugs and Crime (UNODC). 2021. Presentasi *Counter Proliferation Financing* (CPF): *International Obligations and CPF in Operation*.

United States Department of the Treasury. 2018.*National Proliferation Financing Risk Assessment*. https://home.treasury.gov/system/files/136/2018npfra_12_18.pdf.

2019. Pengkinian Penilaian Risiko Indonesia Terhadap Tindak Pidana Pendanaan Terorisme Tahun 2015 (NRA TPPT 2015 *updated*). https://www.ppatk.go.id//backend/assets/images/publikasi/1573608909_.pdf.

2019. Pengkinian Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang Tahun 2015 (NRA TPPU 2015 *updated*). https://www.ppatk.go.id//backend/assets/images/publikasi/1571199475_.pdf.

2019. Program *Mentoring* Berbasis Risiko (Promensisko) 2019: Kompilasi Pedoman Penanganan Perkara TPPU (Penyidikan-Penuntutan-Pemeriksaan Pengadilan).

2021. Penilaian Risiko Indonesia Terhadap Tindak Pidana Pendanaan Terorisme dan Pendanaan Proliferasi Senjata Pemusnah Massal Tahun 2021.

2021. Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang Tahun 2021.

Tim Penyusun

PENGKINIAN KAJIAN TIPOLOGI TINDAK PIDANA PENCUCIAN UANG, TINDAK PIDANA PENDANAAN TERORISME, DAN PENDANAAN PROLIFERASI SENJATA PEMUSNAH MASSAL TAHUN 2023

PENGARAH
Filianingsih Hendarta – Dicky Kartikoyono – Fitria Irmi Triswati

KOORDINATOR DAN EDITOR UMUM
Elyana K. Widyasari – Ronggo Gundala Yudha

TIM PENYUSUN
Danarto Tri Sasongko – Feronika R. Sipayung – Tita Sylvia Rachma – Nabila Femiliana – Catherine Tania

INSTANSI/LEMBAGA KONTRIBUTOR
Pusat Pelaporan dan Analisis Transaksi Keuangan

PENGOLAH DATA, LAYOUT, DAN PRODUKSI
Alfina Hikmatin Tsamami

DOKUMEN LENGKAP DALAM FORMAT PDF TERSEDIA PADA WEBSITE BANK INDONESIA:
https://www.bi.go.id

PERMINTAAN, KOMENTAR, DAN SARAN HARAP DITUJUKAN KEPADA:
Bank Indonesia
Departemen Kebijakan Sistem Pembayaran
Jl. MH Thamrin No. 2, Jakarta, Indonesia
Email : DKSP-APUPPT@bi.go.id
Contact Center Bank Indonesia (BICARA 131)
Telp 1500131 (dari dalam dan luar negeri), bicara@bi.go.id