Panduan Penerapan Program APU PPT Berbasis Risiko terkait *Business Email Compromise* (BEC)

Grup Penanganan APU PPT
Otoritas Jasa Keuangan
2021

Latar Belakang

Pandemi COVID-19 yang terjadi di seluruh dunia tidak hanya berdampak pada aspek kesehatan dan ekonomi, namun memiliki keterkaitan pula dengan meningkatnya ancaman Tindak Pidana Pencucian Uang (TPPU) dan Tindak Pidana Pendanaan Terorisme (TPPT). Dalam hal ini, berbagai respon dilakukan oleh Pemerintah berbagai negara dalam rangka menanggulangi dampak Pandemi COVID-19, mulai dari bantuan sosial; inisiatif keringanan pajak; pembatasan kegiatan tatap muka; hingga tindakan pembatasan perjalanan dan mobilisasi masyarakat untuk menghindari perluasan penyebaran virus; yang secara tidak langsung dapat memberikan peluang baru bagi pelaku kejahatan dan teroris untuk menggunakan celah dan kesempatan yang ada agar dapat menghasilkan uang dan mencuci hasil kejahatan. Hal tersebut sejalan pula dengan kondisi di era digital saat ini khususnya pada Sektor Jasa Keuangan (SJK) dimana semakin beragamnya produk dan fasilitas keuangan berbasis digital yang disediakan oleh Penyedia Jasa Keuangan (PJK) untuk dapat memberi kemudahan bagi Nasabahnya agar tetap dapat bertransaksi dengan nyaman di masa Pandemi COVID-19. Berdasarkan *COVID-19-related Money Laundering and Terrorist Financing – Risk and Policy Responses* yang disusun oleh *Financial Action Task Force on Money Laundering* (FATF) pada bulan Mei 2020, respon dari Pemerintah atas Pandemi COVID-19 bervariasi sesuai dengan dampak di masing-masing negara. Namun demikian secara umum, Pandemi COVID-19 memberikan dampak sebagai berikut:

1. Pemerintah, bisnis, dan individu beralih ke sistem *online* untuk memungkinkan aktifitas secara jarak jauh. Individu yang berada dalam status "*lockdown*" atau pembatasan lainnya juga beralih ke penggunaan *platform online* untuk interaksi sosial.
2. Bisnis yang diklasifikasikan sebagai non-esensial telah ditutup secara fisik. Baik bisnis esensial maupun non-esensial mengalami peningkatan penjualan secara *online*.
3. Pandemi COVID-19 telah mendorong permintaan pasokan medis yang signifikan, seperti alat pelindung diri, ventilator, dan obat-obatan, serta terjadi kelangkaan barang-barang tersebut secara global karena permintaan yang tinggi.
4. PJK tetap beroperasi dengan menawarkan layanan yang lebih terbatas dan membatasi interaksi secara fisik.
5. Penutupan banyak bisnis karena adanya kebijakan *"lockdown"* atau pembatasan kegiatan lainnya pada aspek perdagangan dan perjalanan yang berdampak pada pengangguran massal dan hilangnya pendapatan pemerintah.

Selain itu, dengan adanya penurunan volume perdagangan global dan pembatasan perjalanan, skema kejahatan terorganisir transnasional yang biasanya menggunakan cara

konvensional, yaitu memanfaatkan *global supply chain,* dan skema kejahatan terorganisir lainnya juga terkena dampak atas Pandemi COVID-19. Berkaitan dengan hal tersebut, telah terjadi peningkatan *cybercrime* yang cukup tajam, diantaranya melalui penipuan *Business Email Compromise* (BEC), *email* dan SMS *phising attacks*, dan *ransomware attacks.* Sejalan dengan hal tersebut, Pengkinian Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang Tahun 2021/*National Risk Assessment* (NRA) TPPU Tahun 2021 telah mengidentifikasi potensi risiko TPPU di masa Pandemi COVID-19, dimana disebutkan bahwa adanya peningkatan layanan transaksi berbasis digital membuat para pelaku kejahatan memanfaatkan situasi dan kondisi, salah satunya terkait kejahatan transfer dana yang berkaitan dengan BEC.

Secara khusus terkait dengan BEC, kondisi aktifitas yang dilakukan secara jarak jauh pada berbagai aspek termasuk dalam hal transaksi keuangan dalam rangka pembayaran jual-beli, dimanfaatkan pelaku kejahatan untuk mengeksploitasi kelemahan keamanan jaringan bisnis secara *online*. Eksploitasi dilakukan dengan cara mengakses kontak Nasabah dan informasi transaksi yang kemudian digunakan untuk mengirimkan *email phishing*. Dengan *email phishing*, pelaku kejahatan berpura-pura sebagai pelaku bisnis dan mengarahkan pembayaran untuk barang/jasa/layanan ke *illicit account* dari pelaku kejahatan. Dalam hal ini, PJK memiliki peran penting dalam mengidentifikasi, mencegah, dan melaporkan skema penipuan BEC, diantaranya melalui pelaksanaan komunikasi dan kolaborasi antara unit Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU PPT), bisnis, pencegahan penipuan, dan *cybersecurity*. PJK diharapkan menjadi lebih teliti dan jeli dalam pelaksanaan *Customer Due Diligence* (CDD) khususnya terhadap nasabah korporasi (*legal person*), mengingat pelaku BEC umumnya adalah korporasi.

Pada panduan ini, akan dibahas upaya memitigasi risiko terjadinya skema penipuan BEC melalui peningkatan penerapan program APU PPT berbasis risiko, yang memuat:

1. Gambaran BEC;
2. Indikator terkait BEC;
3. Tindak lanjut PJK terkait BEC;
4. Contoh kasus terkait BEC; dan
5. Strategi mitigasi risiko yang dapat dilakukan oleh PJK.

1. Gambaran BEC

Berdasarkan publikasi *web* terkait *scams and safety* dari *Federal Bureau of Investigation* (FBI), *Business Email Compromise/Email Account Compromise* (BEC/EAC) adalah penipuan canggih yang menargetkan bisnis dan individu yang melakukan permintaan transfer dana yang sah. Penipuan seringkali dilakukan saat pelaku menyusupi (*compromise*) akun bisnis atau *email* pribadi yang sah melalui rekayasa sosial (*social engineering*) atau teknik intrusi komputer (*computer intrusion*) untuk melakukan transfer dana yang tidak sah. Karakteristik dari BEC adalah sebagai berikut:

1. **Memalsukan akun *email* atau *situs web*.**

   Sedikit variasi pada alamat yang sah sehingga mengelabui korban agar mengira akun palsu tersebut merupakan akun asli.

2. ***Email spearphishing*.**

   Email yang terlihat berasal dari pengirim terpercaya untuk mengelabui korban agar mengungkapkan informasi rahasia.

3. **Menggunakan *malware*.**

   Perangkat lunak berbahaya dapat menyusup ke jaringan perusahaan dan memanen *(harvest)* data termasuk kredensial. Seringkali digunakan dengan meyakinkan karyawan untuk mengklik tautan palsu atau lampiran yang berisi *file*.

1.1. Skema BEC

Sebagaimana pembahasan pada *Egmont Group Bulletin* terkait *Business Email Compromise Fraud* yang diterbitkan pada bulan Juli 2019, Skema BEC umumnya melibatkan peniruan identitas korban untuk menyerahkan instruksi transaksi yang tampak sah untuk dijalankan oleh PJK. Meskipun skema BEC berbeda dalam aspek-aspek tertentu, namun seluruhnya berfokus pada penggunaan akun *email* yang disusupi agar PJK dan/atau Nasabah melakukan pembayaran yang tidak sah untuk mengirim data sensitif ke pihak ketiga yang tidak berwenang, dimana data tersebut digunakan untuk melakukan *financial fraud*. Skema BEC dapat dipecah menjadi tiga tahap:

Tahap 1 – Melakukan Penyusupan atas Informasi Korban dan Akun *Email*:

Pelaku kejahatan secara tidak sah mengakses akun *email* korban, seringkali melalui *social engineering* atau teknik intrusi komputer. Dalam hal ini *social engineering* merupakan teknik interaksi yang biasa digunakan pelaku kejahatan untuk menipu

seseorang agar dapat mengungkapkan informasi pribadinya. Pelaku kejahatan kemudian mengeksploitasi akun *email* yang disusupi untuk mendapatkan informasi tentang PJK korban, detail akun, kontak, dan informasi terkait.

Tahap 2 – Mengirimkan Instruksi Transaksi

Pelaku kejahatan kemudian menggunakan informasi korban yang dicuri untuk mengirim *email* pembayaran palsu atau instruksi transmisi data ke PJK, dengan cara yang seolah-olah berasal dari korban. Untuk tujuan ini, pelaku kejahatan akan menggunakan akun *email* korban yang sebenarnya atau membuat akun *email* palsu yang menyerupai *email* korban. Untuk mendukung instruksi, pelaku kejahatan dapat memberikan dokumen pendukung yang dipalsukan untuk meningkatkan legitimasi.

Tahap 3 – Melakukan Transaksi Tidak Sah

Pelaku kejahatan mengelabui karyawan atau PJK korban untuk melakukan transfer uang yang seolah-olah merupakan transaksi sah. Instruksi transaksi tersebut mengarahkan pembayaran ke rekening pelaku kejahatan di PJK domestik atau asing. PJK di Asia Timur dan Tenggara serta negara-negara Eropa Barat dan Timur adalah tujuan umum untuk transaksi penipuan ini. Namun demikian, pelaku kejahatan sering menyesuaikan strategi mereka sehingga negara tujuan dapat berubah dengan cepat.

1.2. Skenario BEC

Skema BEC seringkali menargetkan PJK atau Nasabah, termasuk bisnis dan individu, yang melakukan transaksi besar melalui PJK, entitas pemberi pinjaman, perusahaan *real estate*, dan firma hukum. Sebagai ilustrasi, skema BEC yang sering terjadi adalah menggunakan bentuk berikut:

Skenario 1 – Penjahat Meniru Nasabah PJK

- Pelaku kejahatan meretas dan menggunakan akun *email* karyawan Perusahaan A untuk mengirim instruksi transfer dana palsu ke PJK yang digunakan oleh Perusahaan A. Berdasarkan permintaan ini, PJK tersebut melakukan transfer dana ke rekening yang telah dikontrol oleh pelaku kejahatan.
- Pada skenario ini, pelaku kejahatan yang menyamar sebagai Nasabah PJK, meminta PJK untuk melakukan transfer dana yang tidak sah.

Skenario 2 – Kriminal Meniru Seorang Eksekutif ("CEO Fraud")

- Pelaku kejahatan meretas dan menggunakan akun *email* eksekutif Perusahaan B untuk mengirim instruksi transfer dana ke karyawan Perusahaan B, yang bertanggung jawab untuk memproses dan mengeluarkan pembayaran.

- Karyawan tersebut, yang meyakini bahwa instruksi *email* eksekutif adalah sah, memerintahkan PJK yang digunakan Perusahaan B untuk melakukan transfer dana.
- Dalam skenario ini, pelaku kejahatan yang menyamar sebagai eksekutif perusahaan menyesatkan karyawan perusahaan untuk secara tidak sengaja mengizinkan transfer dana palsu ke akun yang dikendalikan oleh pelaku kejahatan.
- Variasi lain dari skenario ini dapat mencakup penjahat yang menyamar sebagai eksekutif perusahaan untuk menyesatkan karyawan perusahaan agar mengirimkan informasi terkait pembayaran gaji atau transaksi sensitif yang dapat digunakan penjahat dalam penipuan keuangan di masa depan.

Skenario 3 – Penjahat Meniru Pemasok atau Penyedia Layanan

- Pelaku kejahatan menyamar sebagai salah satu pemasok Perusahaan C atau penyedia layanan profesional (seperti agen real estat atau pengacara) untuk mengirim *email* dan menyampaikan informasi kepada Perusahaan C bahwa pembayaran atau setoran faktur di masa mendatang harus dikirim ke nomor rekening dan lokasi baru.
- Berdasarkan informasi penipuan ini, Perusahaan C memperbarui informasi pembayaran pemasoknya dalam catatan dan mengirimkan instruksi transfer dana baru ke PJK yang digunakan Perusahaan C, yang kemudian mengarahkan pembayaran ke rekening yang dikendalikan oleh pelaku kejahatan.
- Dalam skenario ini, pelaku kejahatan, yang menyamar sebagai pemasok atau penyedia layanan, mengirimkan informasi pembayaran palsu untuk menyesatkan karyawan perusahaan agar mengarahkan transfer dana ke rekening yang dikendalikan oleh pelaku kejahatan tersebut.

Skenario 4 – Pelaku Kejahatan Menargetkan Layanan Real Estat

- Pelaku kejahatan menyusupi akun *email* agen real estat atau individu yang membeli atau menjual real estat, untuk tujuan mengubah instruksi pembayaran dan mengalihkan dana dari transaksi real estat (seperti hasil penjualan, pencairan pinjaman, atau biaya).
- Dalam skenario ini, penjahat menyamar sebagai agen real estat atau *key participant* lainnya dalam transaksi real estat untuk mengirim instruksi pembayaran palsu yang menyesatkan rekanan untuk mengarahkan uang muka atau dana terkait transaksi real estat lainnya ke dalam akun yang dikendalikan oleh pelaku kejahatan.

2. Indikator Terkait BEC

2.1. Indikator Penipuan BEC

Berdasarkan *Egmont Group Bulletin* terkait *Business Email Compromise Fraud* yang diterbitkan pada bulan Juli 2019, keberhasilan dalam mendeteksi dan menghentikan skema BEC memerlukan *review* dan verifikasi yang baik atas instruksi transaksi Nasabah. Mengingat beberapa indikator terkait BEC sebenarnya mencerminkan aktivitas keuangan yang sah, PJK disarankan untuk menggunakan satu indikator saja dalam mengidentifikasikan Transaksi Keuangan Mencurigakan (TKM). Dalam hal ini, PJK harus mempertimbangkan indikator tambahan serta fakta dan keadaan lainnya, seperti aktivitas keuangan Nasabah secara historis; serta apakah Nasabah tersebut telah menunjukkan beberapa indikator, sebelum menentukan suatu transaksi sebagai TKM. Selanjutnya, PJK juga perlu melakukan penyelidikan dan investigasi tambahan apabila dianggap perlu. Indikator berikut dapat mengidentifikasikan skema BEC:

2.1.1. Indikator terkait Rekening Korban

Pola Umum TKM

- Nasabah mengirimkan *email* instruksi transaksi yang mengarahkan pembayaran ke penerima yang diketahui; namun, informasi akun penerima berbeda dari yang digunakan sebelumnya.
- Nasbah mengirimkan *email* instruksi transaksi yang mengarahkan pembayaran ke penerima dimana Nasabah tidak memiliki riwayat pembayaran atau hubungan bisnis yang terdokumentasi. Selain itu, jumlah pembayaran mirip dengan pembayaran yang sebelumnya dikirim dari Nasabah ke penerima lainnya.
- Nasabah mengirim *email* permintaan transaksi pembayaran tambahan setelah terdapat transaksi pembayaran sukses kepada pemasok/*vendor* yang sebelumnya belum pernah digunakan oleh Nasabah. Hal ini konsisten dengan perilaku penjahat yang mencoba melakukan pembayaran tidak sah tambahan setelah mengetahui bahwa pembayaran palsu sebelumnya telah berhasil dilakukan.
- Nasabah mengirim *email* instruksi transaksi yang dimaksudkan untuk menetapkan permintaan transaksi dengan status "*Urgent*", "*Secret*", atau "*Confidential*".

- Nasabah mengirim *email* instruksi transaksi yang memberikan waktu atau kesempatan terbatas kepada PJK untuk mengkonfirmasi keaslian transaksi yang diminta.
- Nasabah mengirimkan *email* instruksi transaksi transfer dana ke rekening PJK asing yang telah didokumentasikan dalam keluhan Nasabah sebagai tujuan transaksi penipuan.
- Instruksi transaksi *email* Nasabah berisi bahasa, waktu, dan jumlah yang berbeda dari instruksi transaksi yang telah diverifikasi sebelumnya.
- Instruksi transaksi berasal dari akun *email* yang sangat mirip dengan akun *email* Nasabah namun telah sedikit diubah dengan menambahkan, mengubah, atau menghapus satu karakter atau lebih.

  Contoh:

***Email* Asli**	***Email* Penipuan**
john-doe@abc.com	john_doe@abc.com john-doe@bcd.com

- Instruksi transaksi berasal dari akun *email* yang sangat mirip dengan akun *email* Nasabah namun telah sedikit diubah dengan menambahkan, mengubah, atau menghapus satu karakter atau lebih.
- PJK menerima instruksi transaksi melalui *email* dari karyawan Nasabah, yang merupakan *newly-authorized person* untuk rekening, atau *authorized person* yang sebelumnya belum pernah mengirim instruksi transfer dana.
- Karyawan atau perwakilan Nasabah mengirimkan *email* instruksi transaksi atas nama Nasabah yang didasarkan pada komunikasi *email* dari eksekutif, pengacara, atau orang yang ditunjuk. Namun, karyawan atau perwakilan Nasabah tidak dapat memverifikasi transaksi dengan eksekutif, pengacara, atau orang yang ditunjuk tersebut.

<u>Yurisdiksi Berisiko Tinggi untuk BEC</u>

- Rekening penerima dimiliki oleh perusahaan luar negeri atau berada pada PJK yang berlokasi di yurisdiksi berisiko Tinggi.

<u>Penggunaan Dokumen atau *Invoice* Palsu</u>

- Pelaku kejahatan mengirimkan dokumen atau *invoice* palsu kepada karyawan korban untuk mengkonfirmasi transaksi. Dokumen tersebut dapat menyertakan dokumen asli yang telah dimodifikasi untuk mengalihkan uang ke rekening pelaku.

2.1.2. Indikator terkait Rekening Pelaku BEC

Pola Umum TKM

- Setelah terdapat *attack* terhadap rekening/perusahaan, dana segera ditarik, ditransfer keluar PJK, atau ditransfer ke beberapa rekening di PJK yang sama.
- PJK menerima instruksi transfer dana ke suatu rekening, namun pada instruksi dimaksud nama penerimanya bukan merupakan pemegang rekening. Hal ini menjadi contoh dimana seorang korban tanpa disadari melakukan transfer dana ke nomor rekening baru yang diberikan oleh pelaku kejahatan yang menyamar sebagai pemasok/vendor yang dikenal, sambil berpikir bahwa rekening baru tersebut adalah milik pemasok/vendor yang dikenal.

Jumlah Transfer

- Jumlah transfer dana yang diterima oleh rekening penerima tidak sesuai dengan profil Nasabah.

Penggunaan *Money Mules*

- Peningkatan secara seketika dalam transaksi dan saldo dari Nasabah perantara dapat mengidentifikasikan potensi sebagai *money mules* dalam skema BEC. Identitas *money mules* digunakan utuk membuka rekening PJK, mendapatkan kartu Bank dengan PIN, kode yang dipersonalisasi, dan akses ke fasilitas pembayaran *online*. *Money mules* harus menyerahkan informasi dan memberikan akses ke anggota lain dari kelompok kriminal terorganisir untuk melakukan kejahatan. *Money mules* biasanya tidak mengetahui gambaran dari kejahatan yang dilakukan dan hanya menerima sejumlah kecil uang untuk jasa yang diberikan. Penjahat biasanya menggunakan *money mules* untuk melakukan skema penipuan terkait BEC. *Money mules* umumnya mempertahankan saldo rendah atau memiliki aktivitas keuangan terbatas sebelum terlibat dalam skema.

2.2. *Operational Alert* dan Indikator TKM Berdasarkan Hasil Pembahasan INTRACNET

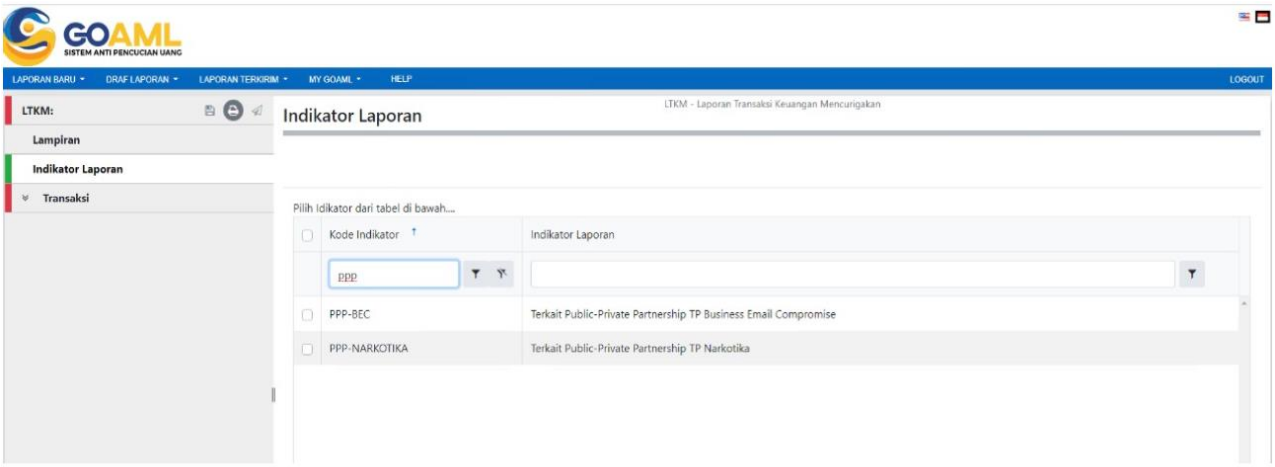
Berdasarkan hasil pembahasan Tim INTRACNET pada Pleno INTRACNET (*Public Private Partnership* Indonesia) dan *Launching Operational Alert* terkait *Business Email Compromise* pada tanggal 25 Agustus 2021, *Operational Alert* BEC yang akan disampaikan kepada seluruh Pihak Pelapor yaitu:

1. Terdapat 1 (satu) atau beberapa transaksi incoming dari luar wilayah Indonesia (misal melalui SWIFT) dengan nominal Rp100.000.000 hingga puluhan miliar Rupiah, kepada pengguna jasa dengan bentuk CV atau PT (biasanya berdomisili di Jabodetabek dan Serang) yang memiliki kesamaan nama dengan perusahaan di luar negeri. CV atau PT dimaksud biasanya juga mencatumkan bentuk badan hukum asing seperti PTE, LTD, PTY, Co.Ltd., LLC, Inc., dll.
2. Usia perusahaan relatif baru didirikan (kurang dari 1 tahun) dan menerima transaksi incoming dari luar wilayah Indonesia dalam waktu yang relatif dekat dengan tanggal pembukaan rekening (biasanya pada hari yang sama atau hingga 1 bulan).
3. Setelah menerima transaksi *incoming*, pengguna jasa melakukan transaksi *outgoing* berupa transfer dana ke luar negeri (misal melalui SWIFT), transfer dana dalam negeri (misal RTGS, kiring, pemindahbukuan) ke beberapa CV atau PT lain yang diduga dikendalikan oleh pelaku/kelompok yang sama, transfer dana ke rekening KUPVA, dan/atau tarik tunai.
4. Transaksi *outgoing* dilakukan pada hari yang sama atau dalam waktu relatif dekat (pass-by, 1-5 hari atau s.d. 1 bulan) dari tanggal transaksi *incoming*, dengan nominal transaksi mencapai ratusan juta hingga milyaran rupiah. Jumlah dana yang keluar dari rekening dapat mencapai 90% dari nominal transaksi *incoming* atau dengan pemecahan transaksi hingga 50 kali.

Selanjutnya, indikator TKM terkait BEC adalah sebagai berikut:

1. Pelaku menggunakan PT atau CV yang memiliki kesamaan nama dengan perusahaan di luar negeri dan mencantumkan bentuk badan hukum asing, serta menggunakan domain *email* yang menyerupai domain *email* perusahaan asing.
2. Pelaku merupakan Warga Negara Asing (WNA) dan berdomisili di luar wilayah Indonesia yang melakukan pengambilalihan perusahaan melalui investasi pada PT atau CV yang sudah berdiri di Indonesia. Pelaku berperan sebagai Pengendali (*Beneficial Owner*) dan identitas pelaku tidak muncul dalam dokumen legalitas yang terdaftar di Kementerian/Lembaga terkait.
3. Pelaku merupakan WNA yang memanfaatkan pihak ketiga dengan kewarganegaraan Indonesia untuk melakukan transaksi. Umumnya pelaku mendampingi, mengarahkan, dan/atau memantau pihak ketiga tersebut dalam melakukan transaksi keuangan.

Lebih lanjut, penyampaian Laporan TKM (LTKM) terkait BEC dapat dilakukan dengan memilih PPP-BEC pada kolom Indikator TKM. Adapun tata cara penyampaian LTKM mengacu pada Peraturan yang dikeluarkan oleh PPATK.



Gambar 1. Pelaporan LTKM terkait BEC pada goAML.

3. Tindak lanjut PJK terkait BEC

3.1. Penundaan Transaksi

Berdasarkan Undang-undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU), PJK dapat melakukan penundaan transaksi dengan rincian sebagai berikut:

Pasal 26 ayat (1)

PJK dapat melakukan penundaan Transaksi paling lama 5 (lima) hari kerja terhitung sejak penundaan Transaksi dilakukan

Pasal 26 ayat (2)

Penundaan Transaksi sebagaimana dimaksud pada ayat (1) dilakukan dalam hal Pengguna Jasa:

a. melakukan Transaksi yang patut diduga menggunakan Harta Kekayaan yang berasal dari hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) UU TPPU;
b. memiliki rekening untuk menampung Harta Kekayaan yang berasal dari hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) UU TPPU; atau
c. diketahui dan/atau patut diduga menggunakan Dokumen palsu.

Pasal 26 ayat (7)

Dalam hal penundaan Transaksi telah dilakukan sampai dengan hari kerja kelima, PJK harus memutuskan akan melaksanakan Transaksi atau menolak Transaksi tersebut.

3.2. Parameter Penundaan Transaksi

Pada Peraturan PPATK Nomor 18 Tahun 2017 tentang Pelaksanaan Penghentian Sementara dan Penundanaan Transaksi oleh PJK, diatur bahwa:

Pasal 13 ayat (1)

Parameter untuk melaksanakan kewenangan melakukan Penundaan Transaksi sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf a (yaitu *melakukan Transaksi yang patut diduga menggunakan Harta Kekayaan yang berasal dari hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) UU TPPU*) dalam hal PJK:

a. menerima laporan atau pengaduan dari Pengguna Jasa atau pihak ketiga yang dirugikan;

b. mendapatkan informasi dari *database* dan manajemen risiko dari PJK;
c. mendapatkan informasi dari Lembaga Pengawas dan Pengatur atau PPATK;
d. mendapatkan informasi dari media massa bahwa Pengguna Jasa diduga melakukan tindak pidana;
e. mendapatkan informasi dari aparat penegak hukum; atau
f. mendapatkan informasi dari sumber lain yang dapat dipertanggungjawabkan kebenarannya.

Pasal 13 ayat (2)

Parameter untuk melaksanakan kewenangan melakukan Penundaan Transaksi sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf b (yaitu *memiliki rekening untuk menampung Harta Kekayaan yang berasal dari hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) UU TPPU*) dalam hal PJK:

a. menerima laporan atau pengaduan dari Pengguna Jasa atau pihak ketiga yang dirugikan dengan melampirkan laporan polisi yang disampaikan oleh Pengguna Jasa atau pihak ketiga yang dirugikan;
b. menerima laporan atau informasi berdasarkan penetapan atau putusan pengadilan;
c. mendapatkan informasi dari database PJK; atau
d. mendapatkan informasi dari sumber lain yang dapat dipertanggungjawabkan kebenarannya.

Pasal 13 ayat (2)

Parameter untuk melaksanakan kewenangan melakukan Penundaan Transaksi sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf c (yaitu *diketahui dan/atau patut diduga menggunakan Dokumen palsu*) dalam hal PJK:

a. mendapatkan informasi dari hasil penelitian atau verifikasi bahwa identitas Pengguna Jasa tidak dikenal atau palsu;
b. mendapatkan informasi bahwa alat transaksi yang digunakan untuk bertransaksi menggunakan nama orang lain atau palsu;
c. mendapatkan informasi adanya penggunaan instrumen pembayaran non tunai palsu; atau
d. mendapatkan informasi dari Dokumen pendukung lain terkait Transaksi.

3.3. Tindak Lanjut Penolakan Transaksi Setelah Lima Hari Kerja

Sebagaimana diatur pada Pasal 26 ayat (7) UU TPPU, dalam hal penundaan Transaksi telah dilakukan sampai dengan hari kerja kelima, PJK harus memutuskan akan melaksanakan Transaksi atau menolak Transaksi tersebut. Terkait dengan tindak lanjut atas hal tersebut, terdapat ketentuan pada Peraturan PPATK Nomor 18 Tahun 2017 tentang Pelaksanaan Penghentian Sementara dan Penundanaan Transaksi oleh PJK, yaitu:

Pasal 14 ayat (7)

Menolak Transaksi sebagaimana dimaksud diatas, meliputi:

a. mengembalikan kepada rekening pengirim;
b. mengembalikan kepada penyetor atau pemilik dana sebagai korban dalam hal penyetoran dilakukan secara tunai; atau
c. tidak melaksanakan Transaksi.

Pasal 14 ayat (8)

Penolakan transaksi sebagaimana dimaksud pada ayat (7) huruf a dan huruf b, dapat dilakukan sepanjang tidak ada permintaan Penghentian Sementara Transaksi dari PPATK atau perintah Penundaan Transaksi dari penyidik, penuntut umum, atau hakim sesuai dengan ketentuan Undang-Undang

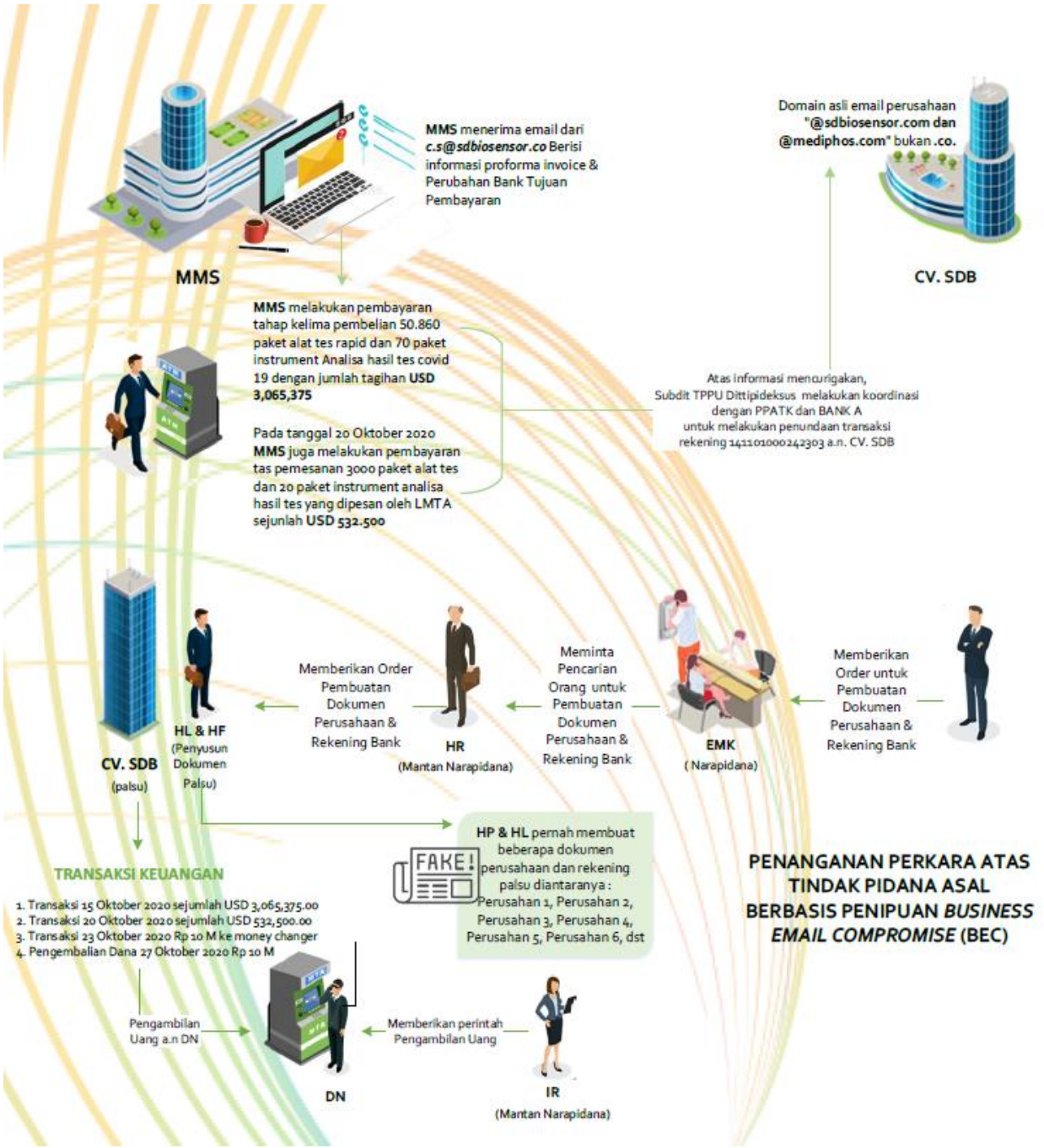
4. Contoh Kasus Terkait BEC

Terdapat 2 kasus terkait BEC yang dipaparkan pada NRA TPPU 2021, yaitu sebagai berikut:

Kasus 1 – Penipuan Berbasis BEC Korban MMS B.V Belanda terkait Kasus Covid-19

- Pelaku kejahatan mengirimkan *email* palsu pada tanggal 14 Oktober 2020 MMS B.V. (MMS) menerima *email* dari c.s@sdbiosensor.co berisi berita informasi proforma *invoice* (faktur sementara) dan perubahan bank tujuan pembayaran ke rekening Bank B an.CV.SD INC untuk pembayaran tahap kelima atas pembelian 50.860 paket alat tes *rapid* dan 70 paket *instrument* ANALISIS hasil tes COVID-19 dengan jumlah tagihan USD 3,065,375. Domain asli *email* perusahaan adalah "@sdbiosensor.com" dan @mediphos.com" bukan.co.
- Pada tanggal 15 Oktober 2020 MMS mentransfer dari Bank C a.n. MMS BV ke Bank R Nomor Rek a.n. CV.SD Inc USD 3,065,375.00 = Rp 44,738 M sesuai dengan Proforma *Invoice* SHJ201009-6 FIN.
- Pada tanggal 20 Oktober 2020 MMS B.V. (MMS) juga melakukan pembayaran atas pemesanan 3.000 paket alat tes dan 20 paket instrument ANALISIS hasil tes yang dipesan oleh LTA dengan total USD 532,500.00 = Rp 7,7 M sesuai dengan Proforma *Invoice* SHJ201016-1 dengan rekening penerima yang sama. Sehingga total transaksi USD 3,597,875.00.
- Atas informasi transaksi mencurigakan tersebut Subdit TPPU Dittipideksus melakukan koordinasi dengan PPATK dan Bank B agar Pihak Bank melakukan penundaan transaksi rekening an.CV.SD INC. Bank B berhasil melakukan penundaan transaksi sejumlah Rp27.832.829.812,- sedangkan dana yang sudah keluar sejumlah Rp24.505.000.000,-
- Penelitian dokumen perusahaan CV.SD Inc terdata pejabat direktur Sdr. HF dan penyelidik dapat menemukan yang bersangkutan dan dilakukan klarifikasi dan didapat informasi bahwa yang bersangkutan mendapatkan order pembuatan dokumen perusahaan dan rekening Bank B dari saudara HR (mantan narapida), hasil pengembangan di lapangan didapat informasi keterlibatan kelompok Nigeria atas nama EMK yang sedang menjalani putusan atas kasus serupa yang disidik oleh Subdit Perbankan Dittipideksus pada tahun 2018.

- Keterangan Tersangka UCNE alias EMK dan koordinasi Kepala Rutan Serang didapat HP Samsung milik EMK di dalam sel rutan. EMK menerangkan bahwa yang bersangkutan mendapat pesanan dari sdr ART (WNA NIGERIA tinggal di kota Enugu) untuk menyiapkan dokumen perusahaan dan rekening perusahaan dengan nama sesuai dengan permintaan ART. Permintaan tersebut dilakukan dengan komunikasi nomor WA. Atas permintaan tersebut EMK meminta sdr HR untuk mencari orang yang bisa membuat dokumen perusahaan dan rekening dan didapat Sdr HL dan Sdr HF. EMK juga pernah meminta membuat dokumen perusahaan dan rekening lainnya.
- Analisis Transaksi Rekening Bank B an. CV.SD tanggal 15 Oktober 2020 sejumlah USD 3,065,375.00 = Rp 44,738 M dan tanggal 20 Oktober 2020 sejumlah USD 532,500.00 = Rp 7,7 M.
- Terdapat Transaksi debet ke rekening *money changer* D tanggal 23 Oktober 2020 Rp 10 M dan tanggal 26 Oktober Rp 10 M. Untuk transaksi tanggal 27 Oktober 2020 Rp 10 M terjadi pengembalian dana.
- Berdasarkan hasil analisis diketahui bahwa pembelian valas pada tanggal tersebut dan yang mengambil uang USD atas nama DN dimana saat mengambil uang DN menunjukkan foto dengan menggunakan HP milik DN berupa foto dokumen NPWP CV SD, foto slip transfer dari rekening SD, foto KTP an. HI.
- Penyidik melakukan penangkapan terhadap Sdr DN dan didapat identitas asli yaitu BA, selanjutnya dilakukan penangkapan dan penahanan atas TSK BA alias DN. Keterangan TSK BN bahwa yang bersangkutan mendapatkan perintah untuk mengambil uang dari Sdri NA alias IR (mantan narapida kasus BEC yang sedang proses penyidikan oleh Kepolisian RI Bareskrim tahun 2019) dan menyerahkan uang valuta asing kepada WNA Nigeria yang tidak dikenal di Indonesia.

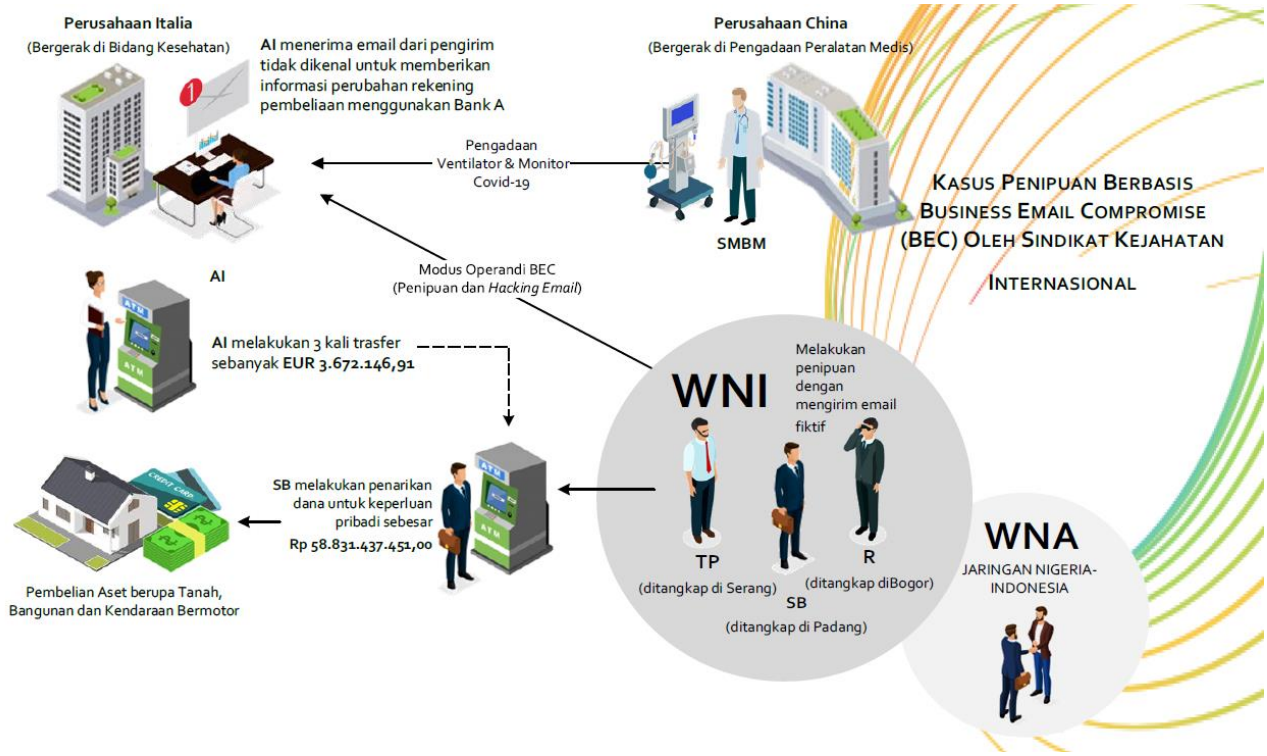


Gambar 2. Skema BEC Kasus 1.

Kasus 2 – Kasus Penipuan Berbasis BEC Oleh Sindikat Kejahatan Internasional Terkait Pembelian Ventilator dan Monitor COVID-19

- Perkara dugaan Tindak Pidana Penipuan atau Tindak Pidana Pemalsuan atau Tindak Pidana Transfer Dana dan atau Tindak Pidana ITE dan Tindak Pidana Pencucian Uang yang dilakukan oleh CV. SMBME. LTD., dkk. yang terjadi dari periode 6 Mei 2020 sampai dengan 22 Mei 2020 dengan modus BEC dalam transaksi jual beli Ventilator dan Monitor COVID-19 antara Perusahaan Italia (AA S.p.A) dengan Perusahaan China (SMBME Co., Ltd.). Para tersangka mengaku sebagai pihak penjual alat medis dan menyuruh korban untuk mengirim sejumlah uang sesuai dengan kesepakatan ke rekening Bank SM yang ada di Indonesia.
- Pada tanggal 31 Maret 2020 perusahaan Italia yang bergerak di bidang peralatan kesehatan a.n. AA S.p.a melakukan kontrak jual beli dengan perusahaan China a.n. SMBME Co., Ltd. untuk pengadaan peralatan medis berupa Ventilator dan Monitor COVID-19, dengan pembayaran beberapa kali ke rekening Bank CH atas nama SMBME., Ltd.
- Pada tanggal 6 Mei 2020 pihak yang tidak dikenal mengirim email kepada perusahaan a.n. AAS.p.a dengan memperkenalkan diri sebagai General Manager (GM) SMBEM Co., Ltd. di Eropa dan memberikan informasi terkait perubahan rekening penerima pembayaran atas pembelian peralatan medis Ventilator dan Monitor COVID-19 yang di pesan, rekening tersebut adalah rekening atas nama CV. SMBME CO. LTD menggunakan bank di Indonesia.
- NCB Interpol Indonesia mendapatkan informasi dugaan tindak pidana penipuan dari NCB Interpol Italia yang mana selanjutnya diteruskan kepada Subdit TPPU Dittipideksus Bareskrim Polri, dari informasi yang diterima tindak pidana dilakukan oleh sindikat kejahatan internasional jaringan Nigeria-Indonesia dengan modus operandi BEC (*Business Email Compromise*) terhadap perusahaan a.n. AA S.p.a dimana korban sudah melakukan 3 (tiga) kali transfer dana ke Rekening Bank SM dengan total EUR 3.672.146,91 atau setara dengan Rp58.831.437.451,00.
- Subdit TPPU Dittipideksus Bareskrim Polri, NCB Interpol Indonesia, dan NCB Interpol Italia berhasil mengungkap sindikat penipuan internasional yang melibatkan jaringan Nigeria dan 2 (dua) pelaku dari Indonesia terkait tindak pidana pencucian uang dengan modus operandi *hacking email*, dan penipuan. Pelaku yang terdiri dari dari "SB" (WNI) ditangkap oleh tim gabungan Bareskrim Polri, Polda Sumut dan Polres Simalungun di Padang Sidempuan, Sumatera Utara.

- Subdit TPPU Dittipideksus Bareskrim Polri sudah melakukan penangkapan terhadap 3 (tiga) pelaku WNI yang bertugas untuk menyiapkan dokumen perusahaan dan rekening perusahaan SMC fiktif yang ada di Indonesia. Pelaku "SB" (WNI) ditangkap oleh tim gabungan Subdit TPPU Dittipideksus Bareskrim Polri, Polda Sumut dan Polres Simalungun di Padang Sidempuan, Sumatera Utara. Dari hasil penangkapan "SB" terungkap fakta bahwa ada keterlibatan pelaku WNI lain, yakni "R" yang terlibat dalam perencanaan dan pembuatan dokumen untuk melancarkan penipuan ditangkap di Bogor, Jawa Barat dan "TP" yang juga terlibat dalam perencanaan dan pembuatan dokumen untuk melancarkan penipuan ditangkap di Serang, Banten.
- Dari kerugian Rp58.831.437.451,00 sudah berhasil ditarik dan dipergunakan oleh tersangka "SB" untuk keperluan pribadi. Tim gabungan Bareskrim dan NCB Interpol Indonesia saat ini masih melakukan pengembangan guna mengungkap pelaku lain yang terlibat, khususnya pelaku yang diduga WNA.



Gambar 3. Skema BEC Kasus 2.

Selanjutnya, berdasarkan *Update: COVID-19-related Money Laundering and Terrorist Financing – Risk and Policy Responses* yang disusun oleh *Financial Action Task Force on Money Laundering* (FATF) pada bulan Desember 2020, terdapat kasus internasional terkait BEC, yaitu sebagai berikut:

Kasus 3 – Kasus BEC Internasional: Singapura dan Perancis.

Penipuan Berbasis BEC Oleh Sindikat Kejahatan Internasional Terkait Pembelian Ventilator dan Monitor COVID-19

- Pada Maret 2020, sebuah Bank yang berbasis di Singapura mengeluarkan *alert* setelah menerima dana berdasarkam pesan dari Perusahaan Prancis. Bank tersebut memberi tahu Otoritas Singapura atas adanya *alert* tersebut, mengingat transaksi terkait dengan *counterpart* internasional. Otoritas Singapura segera memberi tahu Perancis terkait dengan aliran dana yang mencurigakan dan adanya kemungkinan penipuan.
- Melalui intervensi yang cepat dan kolaborasi dengan bank, Kepolisian Singapura menyita lebih dari SGD 6,4 juta (EUR 4 juta) pada hari yang sama dengan adanya *alert* dari Bank.
- Penyelidikan berikutnya menemukan bahwa Perusahaan Perancis yang bergerak pada bidang farmasi menjadi korban penipuan yang melibatkan perintah transfer palsu dengan kerugian total sebesar EUR 6,64 juta.
- Perusahaan melakukan pemesanan masker bedah dan *hand sanitirzer* dari pemasok biasa mereka, yang identitasnya dicuri melalui penipuan BEC. Perusahaan Perancis tertipu mentransfer EUR 6,64 juta ke rekening Bank yang berbasis di Singapura yang dimiliki oleh penipu, setelah itu perusahaan tidak menerima produk atau tidak dapat menghubungi pemasok.
- Kemudian pada bulan Maret 2020, seorang pria berusia 39 tahun ditangkap di Singapura karena kerucigaan atas hasil penipuan pencucian uang terkait persediaan medis untuk COVID-19 sebesar SGD 10,2 juta (EUR 6,64 juta). Sampai dengan Desember 2020, pria tersebut belum didakwa. Pelaku ditemukan bertindak bersama-sama dengan kelompok kejahatan terorganisir yang berbasis luar negeri. Pihak berwenang Singapura terus bekerja sama dengan pihak berwenang Perancis atas kasus tersebut.

5. Strategi Mitigasi Risiko oleh PJK

Berdasarkan uraian tersebut, dalam rangka memitigasi risiko terjadinya BEC, PJK di Sektor Perbankan, Pasar Modal, dan IKNB perlu menyusun kebijakan dan prosedur serta mitigasi risiko yang memadai. Hal-hal yang dapat dilakukan antara lain:

Identifikasi dan Mitigasi Risiko

1. PJK wajib melakukan identifikasi, penilaian, dan mitigasi risiko TPPU termasuk yang berasal dari BEC serta memastikan upaya mitigasi berdasarkan hasil identifikasi risiko tersebut telah dilakukan.
2. PJK agar melakukan proses pengumpulan informasi tambahan terkait perkembangan tipologi *cybercrime* (pada umumnya) dan BEC (khususnya).
3. PJK agar memiliki sistem manajemen risiko yang memadai untuk dapat memitigasi terjadinya *cybercrime* termasuk BEC.

Kebijakan dan Prosedur

4. PJK wajib menyusun, me*review*, mengkinikan, dan memastikan penerapan kebijakan dan prosedur terkait pengelolaan dan mitigasi risiko TPPU yang berasal dari *cybercrime.*
5. PJK wajib memiliki pedoman untuk melakukan penolakan transaksi/pembatalan transaksi/penundaan transaksi/penutupan hubungan usaha dengan Nasabah yang terkait dengan *cybercrime.*

Identifikasi dan Verifikasi Nasabah

6. PJK wajib melakukan verifikasi keaslian informasi yang disampaikan, terutama pada saat melakukan transaksi dan pembukaan rekening. Dalam hal ini, PJK dapat memverifikasi keaslian instruksi pembayaran transaksi *email* yang mencurigakan dengan berkomunikasi dengan Nasabah melalui berbagai cara (misalnya, telepon, akun *email* alternatif), atau dengan menghubungi orang lain di perusahaan Nasabah yang berwenang untuk melakukan transaksi.
7. **PJK wajib melakukan *Customer Due Diligence* (CDD) dan *Enhanced Due Diligence* (EDD) secara memadai khususnya terhadap Nasabah Korporasi atau *legal person*, mengingat pelaku skema BEC seringkali merupakan kelompok kriminal terorganisir yang berkedok korporasi.**

***Monitoring* dan Evaluasi**

8. PJK wajib melakukan *monitoring* berkala terhadap Nasabah, transaksi, termasuk untuk mengidentifikasi pihak *counterparty* yang bertransaksi dengan Nasabah tersebut, serta melakukan pengkinian parameter *monitoring* untuk memastikan sistem *monitoring* memadai dan sesuai tipologi terkini.
9. PJK wajib melakukan evaluasi pola transaksi dengan profil Nasabah secara berkala, parameter *red flag*, termasuk indikator *high risk countries*.
10. PJK agar mengidentifikasi TKM dan Nasabah berisiko Tinggi dengan menggunakan prinsip *Risk Based Approach* (RBA).

Penundaan Transaksi dan Pelaporan LTKM

11. PJK agar mengidentifikasi dan melaporkan TKM dengan pendekatan berbasis risiko serta melakukan penundaan transaksi dan pelaporan TKM secara proaktif, ketika menerima notifikasi dugaan terjadinya *fraud*, diantaranya terkait permintaan pengembalian dana dari bank pengirim atau notifikasi dari PPATK.

Pengawasan Internal

12. PJK wajib melakukan audit internal secara berkelanjutan untuk memastikan pemenuhan seluruh ketentuan/kebijakan dan prosedur.

SDM dan Pelatihan

13. PJK agar melaksanakan pelatihan yang memasukkan materi tipologi BEC/*cybercrime*.
14. PJK agar memastikan pegawai yang terkait dengan penerapan program APU PPT khususnya yang berkaitan langsung dengan Nasabah dan/atau transaksi Nasabah termasuk Satuan Kerja Audit Internal memiliki pemahaman yang memadai terkait dengan APU PPT dan BEC/*cybercrime*.

Perhatian khusus: Transfer Dana dari dan Ke Luar Negeri

15. PJK wajib melakukan CDD/EDD terhadap Nasabah yang menerima transfer dari luar negeri dalam jumlah signifikan di luar pola kebiasaan transaksi.
16. PJK agar menyusun, me*review*, dan memastikan penerapan *Standard Operating Procedure* (SOP) terkait transfer dana untuk memitigasi risiko terjadinya skema BEC.

Daftar Pustaka

Tim Pelaksana NRA TPPU. 2021. Pengkinian Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang Tahun 2021. Jakarta: PPATK.

FATF. 2020. *COVID-19-related Money Laundering and Terrorist Financing – Risk and Policy Responses* FATF. Paris: FATF *Secretariat.*

_____. 2020. *Update: COVID-19-related Money Laundering and Terrorist Financing – Risk and Policy Responses* FATF. Paris: FATF *Secretariat.*

Peraturan PPATK Nomor 18 Tahun 2017 tentang Pelaksanaan Penghentian Sementara dan Penundanaan Transaksi oleh PJK.

Undang-undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Egmont Group. 2019. *Business Email Compromise Fraud*, *Bulletin-01*: 2-7.

FBI. *Business Email Compromise.* (https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-*email*-compromise, diakses tanggal 15 September 2021).