

**KEBIJAKAN DALAM PENANGGULANGAN
PENYALAHGUNAAN KARTU KREDIT¹
Oleh: Hendryawan Dwi Putra Idris²**

ABSTRAK

Tujuan dilakukannya penelitian ini yaitu untuk mengetahui bagaimanakah modus operandi tindak pidana penyalahgunaan kartu kredit dan bagaimanakah kebijakan hukum pidana untuk dalam upaya penanggulangan tindak pidana penyalahgunaan kartu kredit menurut hukum positif Indonesia, di mana dengan menggunakan metode penelitian hukum normatif disimpulkan bahwa: 1. Modus operandi kejahatan kartu kredit atau *carding* ada bermacam-macam yakni: *fraud application, non received card, lost/stollen card, altered card, totally counterfeiled, white plastic card, record of charge pumping, altered amount, telephon/mail ordered*, mengubah program *electronic data/draft capture dan fictius merchant*. 2. Kebijakan hukum pidana dalam upaya menanggulangi tindak pidana dengan menggunakan kartu kredit atau kejahatan kartu kredit atau *carding* dilakukan dengan menggunakan sarana penal yaitu penerapan Pasal 362, 378 dan 263 ayat (1) KUHP dan Pasal 32 ayat (1) UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan upaya non penal yaitu melakukan sosialisasi ke masyarakat tentang kejahatan kartu kredit dan dampaknya bagi pengguna kartu kredit. Selain itu juga dilakukan upaya penanggulangan *carding* secara preventif, dimana Kepolisian merekomendasikan kepada Bank Indonesia untuk melakukan pengawasan/pembatasan terhadap peredaran/penerbitan kartu kredit, menerbitkan buku merah tentang panduan pencegahan dan penanggulangan *carding* dan Bank Indonesia membentuk regulasi yang mengatur penggunaan kartu kredit sebagai pencegahan terjadinya *carding*. Untuk upaya penanggulangan secara represif, dilakukan upaya mediasi anatar pihak bank yang mengeluarkan kartu kredit, pemegang kartu kredit dan pelaku *carding* dengan mediator Bank Indonesia. Apabila tidak tercapai, pelaku

diserahkan kepada Kepolisian untuk ditangani seperti kejahatan lainnya.

Kata kunci: kartu kredit;

PENDAHULUAN

A. Latar Belakang

Seiring dengan pertumbuhan penggunaan kartu kredit tersebut, timbul penyalahgunaan dengan berbagai *modus operandi* yang menimbulkan kerugian tidak saja bagi perbankan khususnya Penerbit kartu kredit, tetapi juga bagi masyarakat pengguna kartu kredit itu sendiri dan kerugian tersebut menunjukkan angka yang terus meningkat secara tajam. Tindak pidana yang berhubungan dengan kartu kredit, pada umumnya dilakukan dengan penuh perhitungan serta menggunakan perangkat pengetahuan yang dimiliki oleh pelakunya, karena para pelaku tindak pidana tersebut pada umumnya terdiri dari orang-orang atau golongan masyarakat yang memiliki tingkat kecerdasan yang relatif tinggi serta mampu memanfaatkan kemajuan teknologi. Akibatnya *modus operandi* tindak pidana yang berhubungan dengan kartu kredit semakin sempurna dan bervariasi serta tidak jarang menimbulkan kesulitan dalam penyidikannya.

B. Rumusan Masalah

1. Bagaimanakah modus operandi tindak pidana penyalahgunaan kartu kredit?
2. Bagaimanakah kebijakan hukum pidana untuk dalam upaya penanggulangan tindak pidana penyalahgunaan kartu kredit menurut hukum positif Indonesia?

C. Metode Penelitian

Metode penelitian yang digunakan adalah metode penelitian kepustakaan.

PEMBAHASAN

A. Modus Operandi Kejahatan Kartu Kredit

Menurut Ade Ary Syam Indradi dalam bukunya "*Carding: Modus Operandi, Penyidikan Dan Penindakan*", modus operandi kejahatan *carding* terdiri dari empat langkah sebagai berikut:

1. Menentukan lokasi akses internet;
2. Memperoleh nomor kartu kredit;
3. Memesan barang;

¹ Artikel Skripsi. Dosen Pembimbing: Frans Maramis, SH, MH; Tonny Rompis, SH, MH

² Mahasiswa pada Fakultas Hukum Unsrat, NIM. NIM. 15071101401

4. Mengirim dan mengambil barang.³

Modus-modus operandi di atas akan dijelaskan sebagai berikut di bawah ini.

1. Menentukan lokasi akses internet;

Langkah awal seorang *carder* untuk beraksi, dimulai dengan menentukan lokasi internet. Seorang *carder* yang akan melakukan kegiatannya, biasanya memilih tempat yang aman.

Apabila dilihat di beberapa *chat room* yang menjadi media berkumpulnya para *carder*, biasanya aktivitas *carder* lebih sering dilakukan pada malam hari hingga menjelang pagi hari. Hal ini karena keberhasilan pemesanan barang terdapat pada jam-jam tersebut. Alasannya, para petugas yang mengurus transaksi *on-line* cenderung lengah dan mereka biasanya langsung memproses transaksi yang masuk tanpa mengecek kemabli apakah kartu kredit yang dipakai sesuai atau tidak.

2. Memperoleh nomor kartu kredit;

Alat pembayaran yang diperlukan dalam bertransaksi *on-line* adalah kartu kredit. Hal yang paling dibutuhkan dari kartu kredit adalah nomor kartu kredit yang terdiri dari 16 digit yang tertera pada sisi bagian depan dan 3-4 digit CCV (*Credit Card Verification*) yang tertera pada sisi bagian belakang, beserta *expired date* kartu. Kedua komponen tersebut, yaitu nomor kartu dan *expire date* kartu adalah komponen terpenting yang dibutuhkan para *carder* dalam bertransaksi *on-line*.

Untuk mendapatkan nomor kartu kredit, maka ada dua metode/cara yang dilakukan para *carder*, yaitu: pertama, memonitor informasi pada *chat-room*. Cara ini mudah dilakukan. Di beberapa *chat-room* secara berkesinambungan dan terjadwal para *carder* memberikan nomor kartu kredit yang cukup banyak. Di antara para *carder* sering saling memberikan informasi atau saling tukar nomor

kartu kredit yang mereka dapatkan di *chat-room*. Kedua, menggunakan *software* generator nomor kartu kredit (melakukan *generate*). *Software* mudah didapatkan dengan *download* dari beberapa situs para *carder*. *Software* ini memudahkan *carder* mendapatkan nomor kartu kredit, *card issue-bank* yang mengeluarkan, area alamat pemegang kartu kredit yang diidentifikasi dengan kombinasi nomor kartu kredit yang mengarah pada kode pos. Penggunaan *software* ini dapat membuat nama, alamat, nomor telepon pemilik kartu secara fiktif. Tetapi perlu ketekunan seorang *carder* untuk mengecek validitas nomor kartu.

Card generator adalah suatu program untuk memperbanyak nomor kartu kredit dari satu nomor induk ataupun tidak. Nomor kartu kredit biasanya diperoleh dari internet.

3. Memesan barang (teknik Order);

Langkah ini dilakukan setelah dua tahapan di atas sudah dilakukan. Modus operandi pemesanan barang melalui internet biasanya dilakukan dengan dua cara, yaitu pertama, *on-line order*; cara ini disebut *web based order* yang merupakan cara umum, tidak terlalu sulit dan paling sering dipakai para *carder*. Pemesanan melalui website dan mengisi form yang disediakan pada website tersebut. Kedua, *e-mail order*; maksudnya adalah *carder* memesan barang dengan mengirimkan *e-mail* kepada *webmaster* dari *merchant* dengan dalih bahwa pemilik kartu kredit tidak mempercayai sistem transaksi melalui *website*, alasan rasa takut nomor kartu kreditnya akan diketahui orang, atau juga alasan alamat tujuan mereka tidak terdapat dalam formulir pengiriman barang. Hal ini dilakukan karena *merchant* (pemilik toko) biasanya tidak hanya melayani transaksi *on-line order* tetapi juga beberapa jenis transaksi lainnya seperti *e-mail order* dan *phone order*. Cara ini dilakukan apabila *carder* lancar memiliki kemampuan menulis atau berkomunikasi menggunakan

³ Ade Ary Syam Indradi, *Carding: Modus Operandi, Penyidikan Dan Penindakan*, Grafika Indah, Jakarta, 2006, hlm. 63.

bahasa Inggris. *E-mail* order dimanfaatkan bagi situs yang tidak menyediakan transaksi *website* sebagai galeri atau tidak memberi pilihan untuk pengiriman ke luar negeri, ke Asia apalagi Indonesia.

4. Mengirim dan Mengambil barang;

Proses ini merupakan tahap akhir proses *carding*. Pengiriman barang hasil transaksi di internet dilakukan beberapa pihak, antara lain kantor pos atau jasa pengiriman barang swasta lainnya. Pemilihan bentuk pengiriman barang biasanya dilakukan pihak *merchant*. Pada saat berkomunikasi dengan *merchant via e-mail*, para *carder* meminta beberapa hal, antara lain: pertama, *removal tag*, yaitu agar penjual mencopot semua label yang terkait dengan harga agar pihak bea-cukai kesulitan memberikan estimasi pajak berdasarkan harga barang, sehingga biaya pajak bisa dinegosiasikan atau bahkan ditiadakan. Bisa juga, barang tersebut diakui sebagai barang bekas, hadiah atau pengiriman kembali karena komplain. Kedua, pengepakan. Permintaan cara pengepakan merupakan siasat mengelabui pihak petugas bea-cukai agar pajak dan asuransinya menjadi lebih murah, misalnya mengepak perhiasan dalam boneka atau membungkusnya bersama buku bekas. Ketiga, permintaan *track number*. Nomor ini diminta untuk mengetahui jalur perjalanan barang. Pada jasa pengiriman tertentu, pelanggannya bisa mengetahui sampai dimana proses pengiriman yang dilakukan, yaitu dengan memasukkan *track number* dari pengiriman pada fitur pencarian barang secara *on-line* pada situs jasa pengiriman yang bersangkutan.

Dari Buku Petunjuk Lapangan “Penyidikan Tindak Pidana Yang Berhubungan Dengan Kartu Kredit”, yang dikeluarkan oleh Markas Besar Kepolisian Negara Republik Indonesia, bentuk atau cara penyalahgunaan kartu kredit yang pernah terjadi adalah sebagai berikut :

1. Menggunakan kartu kredit :

a. Menggunakan kartu asli :

- *Fraud Application*
- *Non Received Card*
- *Lost/Stolen*

b. Menggunakan kartu palsu

- Palsu Sebagian / *Altered Card (Re-embossed / Re-encoded)*
- Palsu Seluruhnya (*Total Counterfeit*)
- *White Plastic Card*

2. Menggunakan *Sales Draft*

- a. Penggantian *Sales Draft (R. O. C. Pumping)*
- b. Merubah Nilai Nominal (*Altered Amount*)

3. Lain-lain

- a. *Mail Ordered / Telephone ordered*
- b. Merubah program EDC
- c. *Merchant Fiktif*⁴

Adapun uraian dari Modus Operandi tersebut di atas adalah sebagai berikut :⁵

1. Modus Operandi *Fraud Application* (Menggunakan kartu yang asli yang diperoleh dengan aplikasi / data palsu)

Pelaku memalsu biodata antara lain : KTP (alamat), pasport, rekening koran, surat keterangan penghasilan dan referensi, lalu melamar kepada Penerbit untuk mendapatkan kartu kredit. Setelah berhasil diterima sebagai Pemegang kartu kredit, selanjutnya melakukan transaksi berkali-kali yang nilainya makin lama makin besar dan tiba-tiba melarikan diri atau menghilang tanpa memenuhi kewajibannya sebagai Pemegang kartu kredit yaitu membayar pemakaian kartu kreditnya.

Salah satu contoh kasus menggunakan modus ini adalah sebagai berikut :

Tuan X memalsukan KTP dengan menggunakan alamat Jalan Seni Suara II no. 57 Jakarta Barat dan menyewa ruangan untuk *show room* mobil di jalan Gunung Salak no. 47 B Jakarta dengan nama PT. Daya Motor, lalu mengajukan aplikasi untuk mendapatkan kartu kredit Bank A dengan limit Rp. 20.000.000. Enam bulan pertama *Cardholder* membayar tepat waktu atas kartu kreditnya ke Bank A dan pada bulan ke tujuh, *Cardholder* berbelanja

⁴ Markas Besar Kepolisian Negara Republik Indonesia, *Op-Cit*, hlm. 35.

⁵ Sigid Suseno dan Syarif A Barmawi, *Op-Cit*, hlm. 254

menghabiskan *credit limit* seluruhnya dan masih berbelanja lagi di bawah *floor limit* untuk menghindari otorisasi, sehingga total tagihan sejumlah Rp. 40.000.000. Ketika pihak Bank A menagih ke kantor yang bersangkutan ternyata sudah kosong dan dioperasikan oleh orang lain. Kemudian pengecekan dilakukan ke rumah yang bersangkutan dan ternyata rumah sudah kosong, dimana rumah tersebut merupakan kontrakan yang diperpanjang setiap bulan.

2. Modus Operandi *Non Received Card* (menggunakan kartu asli yang tidak diterima oleh pemegang kartu sesungguhnya)⁶

Modus ini terjadi karena peluang yang berkaitan dengan pengiriman kartu kredit, dimana kartu kredit yang dikirim oleh Penerbit tidak sampai pada Pemegang dan digunakan oleh orang yang tidak berhak. Dalam prakteknya pelaku membubuhkan tanda-tangan di kolom tanda-tangan (*signature panel*) yang masih kosong dan melakukan transaksi di toko-toko dengan menanda-tangani *sales draft* dan bertindak seolah-olah sebagai Pemegang kartu kredit yang sah.

Dalam pengiriman kartu kredit, semua Penerbit di Indonesia menggunakan kurir atau pihak ke tiga untuk mengirimkan kartu kreditnya. Di luar negeri, Amerika Serikat contohnya, pengiriman kartu dilakukan melalui Pos sehingga untuk menangani pencurian benda-benda pos dibentuk Polisi Khusus yaitu *US Postal Service*. Karena menyangkut pihak ketiga inilah, maka sering terjadi penyalahgunaan seperti hilang di jalan, diberikan pada orang yang tidak berhak atau salah pengiriman, sehingga akhirnya digunakan oleh orang-orang yang mengerti cara menggunakan kartu kredit tersebut.

Salah satu contoh kasus yang pernah terjadi dengan menggunakan modus ini adalah sebagai berikut : Pelaku yang sering tertangkap untuk kasus *non received* ini adalah Tuan Y (tertangkap 3 kali). Dari pengakuan pelaku, kartu kredit diperoleh dari salah seorang temannya yang bernama Mister X yang bekerja sama dengan sindikat pencuri benda-benda pos di Amerika Serikat.

⁶ *Ibid.*

Kartu kredit tersebut biasanya diserahkan oleh Mister X di Singapura dan segera digunakan di Indonesia. Pelaku tertangkap karena kecurigaan kasir setelah melihat nama kartu yang tercetak etnik Amerika sedangkan yang berbelanja berwajah China. Setelah dikonfirmasi kepada Penerbit kartunya, ternyata Pemegang kartu kredit itu berada di Amerika Serikat dan kartu tersebut adalah kartu asli yang tidak sampai kepada pemiliknya.

3. Modus Operandi *Lost / Stolen* (menggunakan kartu asli hasil curian)⁷

Pelaku menggunakan kartu hilang / curian dengan jumlah dibawah *floor limit* dan meniru tanda tangan si pemilik. Biasanya kartu-kartu tersebut dipakai di supermarket atau di Departement Store. Pelaku mendapatkan kartu kredit dari pencopet / penadah dan menggunakannya dengan cara-cara memecah-mecah nilai belanja (*split charge*) agar nilainya di bawah limit sehingga tidak perlu dilakukan otorisasi. Pelaku sangat khawatir bila kartu kredit diotrisasikan karena secara sistem, nomor kartu tersebut telah di blokir sehingga bila di otrisasikan akan keluar perintah *Pick up lost* atau *pick up stolen* dimana pelaku harus ditahan.

Salah satu kasus yang pernah terjadi dengan menggunakan modus ini adalah sebagai berikut: Pada awal tahun 1992 diterima laporan kehilangan kartu kredit Bank M a/n Nyonya R yang ternyata diketahui dipergunakan oleh seorang wanita yang bernama nona T di daerah Bandung dan sekitarnya. Dikarenakan kartu tersebut pernah dilaporkan hilang, maka saat dilakukan transaksi oleh nona T diketahui bahwa kartu kredit a/n Nyonya R disalahgunakan. Pada saat transaksi itu berlangsung, pelaku ditangkap dan dari hasil pengakuan tersangka, diperoleh keterangan bahwa pelaku mendapatkan kartu kredit tersebut dari seorang yang bernama H dengan cara membeli dimana kartu kredit regular/klasik seharga Rp. 100.000 s/d Rp. 300.000 dan kartu gold seharga Rp. 500.000 s/d Rp. 700.000. Untuk melakukan transaksi ini pelaku memalsukan tanda tangan asli (pemegang kartu) yang terdapat dalam

⁷ *Ibid.*

signature panel dan selalu melakukan transaksi di bawah *floor limit merchant* untuk menghindari otorisasi.

4. Modus Operandi *Altered Card* (menggunakan kartu asli yang diubah data)⁸

Pelaku menggunakan kartu asli hasil curian atau pengelapan (*lost/stolen/nonreceived card*) kemudian kartu tersebut reliefnya dipanasi atau diratakan. Setelah rata kemudian relief tersebut dicetak ulang (*re-embossed*) dengan data baru, sedangkan *magnetic stripe* diisi data baru (*re-encoded*), data tersebut didapat dari *Point Of Compromise* (POC) antara lain oknum Pedagang, oknum Bank, teman/orang-orang dekat di lingkungan Pedagang dan biasanya jumlah transaksi besar serta kemungkinan oknum pedagang terlibat.

Salah satu contoh kasus yang pernah terjadi dengan menggunakan modus ini adalah sebagai berikut: Sebuah kartu kredit Bank A dilaporkan hilang a/n Tuan K, kemudian kartu tersebut diratakan dan di *embossed* dengan nama Tuan L dengan nomor kartu Bank H. Kemudian kartu digunakan untuk berbelanja di Matahari Simpang Lima Semarang dengan pelaku bernama S. Dari hasil investigasi, data Tuan K didapat dari *fotocopy sales draft* salah satu *merchant* di Surabaya. Pelaku tertangkap karena kecurigaan kasir terhadap fisik kartu yang tidak sempurna dan segera mengkonfirmasi kepada Bank, sehingga Bank memerintahkan pemilik toko untuk menahan kartu beserta Pemegangnya. Pelaku selanjutnya diserahkan ke Polsek Semarang Timur.

5. Modus Operandi *Totally Counterfeit* (menggunakan kartu kredit yang seluruhnya palsu)⁹

Pelaku mencetak / membuat kartu tiruan bergambar/logo dan fisik 100%

palsu, dibubuhkan data nomor dan nama pemegang kartu yang *bonafid* dan *valid* (masih berlaku). Hal ini dilakukan dengan cara *embossing* dan *encoding*. Jenis kartu ini (total palsu/*non white card*) digunakan sebagaimana asli di Pedagang dengan transaksi yang besar. Biasanya pelaku

sebelumnya berusaha melakukan ujicoba otorisasi. Modus operandi ini dapat berhasil dilakukan karena kartu kredit palsu tersebut mutunya baik dan sangat sulit dibedakan dengan kartu kredit asli atau adanya kerjasama Pemegang kartu dengan oknum Pedagang.

Salah satu contoh kasus yang pernah terjadi dengan menggunakan modus ini adalah sebagai berikut: Kejadian bermula di toko L Duta Merlin, dimana kasir *merchant* tersebut mencurigai fisik kartu yang bertransaksi di toko tersebut dengan logo Bank D, akan tetapi cetakkannya sudah mengelupas. Setelah di cek ternyata nomor kartu berasal dari salah satu Bank di Afrika Selatan. Segera dilakukan penahanan terhadap kartu dan pelakunya diserahkan kepada Polsek Gambir.

6. Modus Operandi *White Plastic Card* (menggunakan kartu kredit polos Yang menggunakan data asli/valid)¹⁰

Modusnya yaitu nomor-nomor yang tercetak timbul pada kartu kredit dicatat lalu dicetak pada kartu plastik polos se ukuran kartu kredit asli, tanpa logo dan tanda-tanda visual lainnya. Selain itu *magnetic stripe* di balik kartu ini, di isi dengan data Pemegang kartu dengan cara *encoding*. Data Pemegang kartu yang sah, didapat dari *Point of Compromise*. Transaksi dengan menggunakan kartu ini, bisa terjadi akibat kerjasama sepenuhnya dengan oknum Pedagang, karena seharusnya kartu polos tersebut tidak dapat digunakan untuk bertransaksi dan selanjutnya *sales-draftnya* ditagihkan kepada pengelola.

Salah satu contoh kasus yang pernah terjadi dengan menggunakan modus ini adalah sebagai berikut: Pada bulan Juni 1992 diketahui bahwa beberapa *merchant* seperti toko Z (Jakarta), toko U, toko D, M Tour & Travel dan Hotel M (Ujung Pandang) telah mengalami lonjakan dalam setoran *merchant*. Dari hasil analisa terhadap setoran *merchant-merchant* tersebut diketahui bahwa 90% dari setoran tersebut dengan menggunakan kartu kredit yang diterbitkan oleh Bank G, Bank H, Bank D *Card Centre*, yang dikonfirmasi kepada pemegang kartu, menyatakan bahwa tidak pernah melakukan

⁸ *Ibid.*

⁹ *Ibid.*

¹⁰ *Ibid.*

transaksi di *merchant-merchant* tersebut. Setelah dilakukan investigasi, ternyata ada kolusi antara *merchant* dengan sindikat kartu kredit karena dari barang bukti yang didapat, adanya 32 buah kartu putih (*white plastic*) yang telah dicetak data Pemegang kartu di atas kartu anggota dari sebuah *Sport Center* di Surabaya yang bernama A Sport Center.

7. Modus Operandi *Record Of Charge Pumping* atau *Multiple Imprint* (penggandaan *sales draft*)¹¹

Oknum Pedagang melakukan pencetakan *sales draft* lebih dari satu kali, selanjutnya *sales draft* hasil penggandaan dijual atau diserahkan kepada oknum *merchant* lainnya untuk diisi dengan data transaksi fiktif, kemudian dibubuhi tanda tangan secara sembarangan atau meniru tanda tangan Pemegang kartu yang sah, baru setelah itu ditagihkan kepada pengelola seolah-olah hasil transaksi yang sebenarnya. Salah satu contoh kasus yang pernah terjadi dengan menggunakan modus ini adalah sebagai berikut: Pada akhir bulan November 1992, Bank C *Card Center* Jakarta khususnya bagian otorisasi menerima permohonan otorisasi melalui facsimile dari salah satu *merchant* bernama "CV X di kota Malang Jawa Timur sebanyak 17 transaksi yang semua kartu kreditnya diterbitkan oleh *Issuer* di luar negeri. Atas kecurigaan tersebut, pihak Bank C *Card Center* mengkonfirmasi transaksi-transaksi tersebut ke *Issuer* di luar negeri, yang ternyata hasil konfirmasi tersebut bahwa Pemegang kartu yang asli tidak pernah melakukan transaksi di *merchant* tersebut di atas.

Berdasarkan hasil konfirmasi tersebut, penyelidikan ke lokasi *merchant* CV X di kota Malang dan hasilnya menyatakan bahwa transaksi yang dilakukan oleh *merchant* tersebut adalah fiktif dan *sales draft* yang ditagihkan ke Bank C *Card Center* merupakan hasil penggandaan *sales draft* atas transaksi yang terjadi pada *merchant* lain yang masih mempunyai hubungan keluarga.

8. *Altered Amount* (mengubah / menambah nilai nominal pada *sales draft*)¹²

Modus ini bisa terjadi dimana oknum Pedagang mengganti nilai nominal yang tercantum pada *sales draft* dari kartu yang digunakan dalam transaksi ditokonya. Misalnya transaksi yang terjadi sebesar Rp. 100.000 diubah menjadi Rp. 1.000.000 dan selanjutnya *sales draft* yang telah diubah ini ditagihkan kepada pengelola.

Salah satu contoh kasus yang pernah terjadi dengan menggunakan modus ini adalah sebagai berikut: Di bulan November 1992, salah satu *merchant* yang bernama toko T diketahui melakukan penambahan jumlah angka transaksi dari beberapa *sales draft* yang disetorkan pada Bank O *Card Center*.

Hal ini diketahui dari sanggahan Pemegang kartu yang menyatakan bahwa Pemegang kartu hanya melakukan transaksi dengan jumlah Rp. 250.000, akan tetapi *sales draft* yang ditagihkan pada Pemegang kartu melalui pengelola kartu kredit (Bank O *Card Center*) sebesar Rp. 2.250.000. Setelah dilakukan penyelidikan pada *merchant* yang bersangkutan, diketahui bahwa oknum pada *merchant* tersebut telah mengubah besarnya jumlah transaksi yang sebenarnya dengan cara menambah angka "2" pada *sales draft* *Bank Copy* yang ditagihkan kepada Bank O *Card Center*.

9. Modus Operandi *Mail Order / Telephone Order* (memesan barang melalui Surat / telepon)¹³

Pelaku melakukan pemesanan suatu barang melalui surat atau telepon dengan memberikan data kartu kredit Pemegang. Modus ini dapat terjadi karena pelaku mengetahui data Pemegang kartu (nama dan nomornya) kemudian pelaku bertidak seolah-olah Pemegang kartu tersebut, memesan beberapa barang pada pedagang yang melayani transaksi melalui telepon / surat, termasuk pengiriman barangnya ke tempat pembeli / pemesan.

Selanjutnya pelaku menerima barang, menandatangani tanda terima dari pedagang di tempat yang ia tentukan sesuai pesanan dan kemudian melarikan diri. Biasanya tempat penerimaan barang atau pesanan adalah alamat palsu.

¹¹ *Ibid.*

¹² *Ibid.*

¹³ *Ibid.*

Salah satu contoh kasus yang pernah terjadi dengan menggunakan modus ini adalah sebagai berikut:

a. *Mail Order*

Seorang sekretaris perusahaan bernama Nyonya B, sering diperintahkan oleh Direkturnya yang bernama Tuan S untuk membayarkan tagihan kartu kreditnya setiap bulan. Ketika melihat ada penawaran pembelian barang melalui surat dengan hanya mencantumkan nomor kartu kredit pembelinya, maka terbersit keinginan Nyonya B untuk memesan barang elektronik untuk dikirimkan ke alamat fiktif dimana pacar Nyonya B sudah menanti untuk menerima barang tersebut. Setelah menerima barang-barang elektronik tersebut, pacar Nyonya B yang bernama Mister A segera menghilang, Sebulan kemudian Tuan S menerima tagihan dari Bank yang sangat besar untuk pembelian barang-barang elektronik dan segera Tuan S melaporkan kepada bank, bahwa dia tidak pernah memesan barang-barang tersebut. Pihak bank segera melakukan pengecekan ke alamat pengiriman yang ternyata sudah kosong ditinggalkan penyewanya.

b. *Telephone Order*

Tuan R seorang pengedar narkotik sekaligus juga penjahat kartu kredit, di penjara selama 4 tahun di negara bagian California karena kasus narkotika. Tuan R mempunyai seorang pacar bernama nona E yang bekerja di sebuah *boutique* di Los Angeles. Setiap pelanggan yang berbelanja di *boutique* tersebut dengan menggunakan kartu kredit, selalu dicatat oleh Nona E ke dalam secarik kertas.

Catatan tersebut diserahkan kepada Tuan R setiap kali ke penjara. Kemudian Tuan R memesan barang melalui telepon pada beberapa *merchant* yang menerima transaksi melalui telepon order, dengan mengaku sebagai *Cardholder* atau Pemegang kartu.

Barang-barang itu diminta dikirimkan ke suatu tempat yang merupakan alamat rekan Tuan R di luar penjara dahulu yaitu Mister D dan merupakan alamat palsu, dimana dalam hal ini Mister D bertindak selaku penadah barang-barang tersebut. Kasus ini terungkap setelah pemegang kartu menolak tagihan bank dan menyatakan tidak pernah memesan barang. Kemudian melaporkan kepada *Secret Service* yang langsung melakukan pelacakan telepon. Dari pelacakan tersebut, akhirnya diketahui bahwa pesanan berasal dari penjara, kemudian langsung dapat ditelusuri siapa pelakunya, ternyata Tuan R.

10. Modus Operandi Mengubah atau Merusak Program *Electronic Data/Draft Capture (EDC)*¹⁴

Modus ini dapat terjadi karena, oknum pedagang mengubah dan merusak program alat otorisasi EDC milik pengelola yang dititipkan, dipinjamkan pada *merchant*. Alat ini direkayasa agar dapat dilakukan otorisasi atau dioperasikan tanpa perlu ada kartu kreditnya secara fisik.

Pelaku disini bertindak seolah-olah ada transaksi normal yang dihadiri oleh Pemegang kartu disertai kartu kreditnya. Namun kenyataannya pelaku/oknum pedagang melakukan sendiri dengan menggunakan kartu-kartu palsu atau langsung secara manual pada EDC dengan memasukkan data Pemegang kartu yang sah (tanpa ada kartunya) yang didapat dari POC atau dari *sales draft* kartu asli yang pernah dipergunakan. Setelah di otorisasikan maka keluarlah persetujuan yang ditandai dengan keluarnya *sales draft* secara otomatis yang kemudian ditandatangani sendiri dan disetorkan pada pengelola.

Salah satu contoh kasus yang pernah terjadi dengan menggunakan modus ini adalah sebagai berikut: Untuk mempermudah proses otorisasi dan peningkatan pelayanan kepada *merchant*, pihak bank meminjamkan suatu alat yang disebut EDC (*Electronic Data/Draft Capture*). Sebuah *merchant* yang bernama toko W (berdagang computer, mesin fax, dan lain-lain) oleh salah sebuah

¹⁴ *Ibid.*

pengelola kartu kredit, diberikan alat EDC. Kecurigaan pihak pengelola mulai timbul, ketika dalam laporan aktifitas toko tersebut (*merchant activity report*) terdapat kode angka 01 pada laporan tersebut, yang berarti kartu tidak diotorisasikan (digesek) melalui alat EDC, tetapi telah dilakukan otorisasi secara manual (tanpa ada kartu dan nomor, otorisasi dapat dibuat secara sembarangan). Seharusnya kode angka yang keluar adalah 02, yang berarti otorisasi dilakukan secara sistem dengan menggunakan kartu kredit dan kode otorisasi dikeluarkan oleh bank secara sistem pula.

11. Modus Operandi *Fictitious Merchant* (berpura-pura menjadi pedagang)¹⁵

Pedagang mengajukan aplikasi untuk menjadi *merchant* suatu bank dengan data palsu, kemudian melakukan transaksi-transaksi dengan modus-modus di atas, seolah-olah terjadi transaksi di tokonya. Biasanya kartu yang digunakan adalah kartu-kartu palsu atau kartu curian yang belum sempat di blokir. Setelah di transaksikan, maka *sales draft* tersebut ditagihkan kepada bank pengelola dimana sesudah dana tersebut di transfer oleh bank, maka pedagang fiktif ini akan menghilang dengan meninggalkan tokonya begitu saja.

Salah satu contoh kasus yang pernah terjadi dengan menggunakan modus ini adalah sebagai berikut: Pada saat pertama kali diresmikan, pusat perbelanjaan M Mall membuat program "*Trade Trial*" yaitu memberikan kesempatan kepada pedagang untuk berjualan selama 3 bulan secara gratis (tidak dikenakan biaya sewa), namun setelah 3 bulan harus segera memberikan keputusan akan membeli atau tidak jadi berjualan di M Mall. Program inilah yang dimanfaatkan oleh pedagang-pedagang gadungan tersebut, yaitu setelah mendapatkan ijin untuk berjualan, mereka mengajukan permohonan untuk menjadi *merchant* kepada bank-bank penerbit kartu kredit.

Setelah diterima menjadi *merchant*, pada bulan pertama mereka menyetorkan kartu-kartu asli, dimana pemegang kartunya benar-benar berbelanja. Tetapi pada bulan berikutnya, mereka segera menyetorkan

transaksi dengan menggunakan kartu-kartu palsu atau transaksi fiktif dan setelah dana dibayarkan oleh pihak bank, maka segera mereka melarikan diri dengan meninggalkan tokonya begitu saja. Biasanya mereka membawa barang-barangnya pada malam hari setelah toko tutup. Pihak bank baru menyadari bahwa transaksi-transaksi dengan menggunakan kartu palsu, setelah satu bulan dimuka karena pihak pemegang kartu yang sesungguhnya baru melaporkan bahwa mereka tidak berbelanja di tempat tersebut, setelah menerima tagihan satu bulan setelah transaksi terjadi.

Modus-modus operandi yang sudah diuraikan di atas satu demi satu, dapat berhasil dilakukan oleh para pelaku kejahatan, dikarenakan adanya perbuatan yang mendukung hal tersebut, yakni :

1. *Split Charge*;
2. *Point of compromise (POC)*.¹⁶

Ke dua perbuatan tersebut, penjelasannya sebagai berikut:

1. *Split Charge*

Adalah cara memecah-mecah nilai transaksi untuk menghindari otorisasi atau jumlah minimal belanja tidak melebihi *floor limit*. Caranya dengan membeli barang-barang yang diperlukan tidak sekaligus, tetapi dipilah-pilah sehingga terdapat beberapa *sales draft* yang nilai nominalnya di bawah *floor limit* dan kredit limitnya tidak terlampaui. Akibatnya transaksi yang dilakukan terhindar dari otorisasi, misalnya transaksi *lost/stolen*, *credit run away* dan *counterfeit card*.

Contoh kasus *Split Charge* :

Kartu kredit Bank B atas nama Tuan A dilaporkan hilang pada tanggal 14 July 1992 dan ternyata pada nota tagihan nomor tersebut , pada tanggal jatuh tempo berisikan tagihan pada beberapa toko dimana masing-masing bersangkutan dan diketahui, jika transaksi tersebut dilakukan dengan cara membagi menjadi beberapa *sales draft* dengan maksud untuk menghindari otorisasi. Hal ini dilakukan oleh *merchant* dengan sadar, karena

¹⁵ *Ibid.*

¹⁶ Markas Besar Kepolisian Negara Republik Indonesia, *Op-Cit*, hlm. 42

merchant melakukan kerjasama dengan sindikat pencuri kartu dan sebelum melakukan transaksi *merchant* tersebut telah memeriksa pada daftar hitam terlebih dahulu.

3. *Point of Compromise (POC)*

Yaitu tempat-tempat dimana data Pemegang kartu yang sah seperti nomor kartu, nama, masa berlaku, didapatkan atau disadap untuk selanjutnya dihimpun untuk diberikan kepada pihak ketiga (sindikatis) untuk disalahgunakan. Ini memungkinkan adanya kartu kredit palsu jenis *Totally Counterfeit*, *White Plastic* dan *Reembossed / Reencoded*.

Contoh kasus POC :

Dari hasil penyelidikan *Security Card* AKKI terhadap kasus kartu palsu yang terjadi tahun 1994, sebagian kasus kartu palsu tersebut, setelah diperiksa transaksi beberapa bulan kebelakang, ternyata Pemegang kartu yang sah, pernah melakukan transaksi yang asli di *merchant* yang bergerak dalam bidang *Night Entertainment* yang bernama G Discotik. Berdasarkan temuan tersebut, maka setelah dilakukan penyelidikan yang lebih detail, diketahui jika setiap kartu kredit asli yang di transaksikan di *merchant* tersebut selang waktu satu sampai dengan dua minggu, terdapat kartu palsu beredar, sehingga asumsi yang diambil adalah G Discotik merupakan POC dari kartu palsu yang ada.

Selain apa yang sudah disebutkan diatas, terdapat kemajuan dalam teknik menyadap data Pemegang, sehingga pemalsuan kartu makin sulit untuk dideteksi. Teknik penyadapan data Pemegang terdiri dari :

a. *Generate Account Number* atau *Credit Master*

Yaitu suatu cara untuk mendapatkan data nomor-nomor kartu kredit dengan menggunakan sebuah program (*software*) tertentu yang telah dirancang khusus. Untuk mendapatkan data nomor-nomor kartu kredit tersebut, pelaku hanya perlu memasukkan satu nomor kartu kredit yang pernah dikeluarkan oleh penerbit (*valid*) ke dalam program tersebut, selanjutnya akan

muncul ratusan kombinasi nomor kartu kredit lain yang dapat digunakan untuk data kartu kredit palsu.

b. *Ghost / Phantom Terminal*

Yaitu suatu cara yang dilakukan untuk menguji nomor kartu kredit yang didapat dari berbagai sumber POC, termasuk juga dari cara *Generate Account Number / Credit Master*. Pengujian ini diperlukan untuk mengetahui apakah nomor kartu kredit yang diperoleh, dapat digunakan untuk bertransaksi, bila dapat maka dibuatlah kartu palsu, namun bila tidak, maka data tersebut akan dibuang. Pengujian ini menggunakan POS yang berasal dari pedagang yang sudah tutup, namun tidak mengembalikan POS sesuai dengan perjanjian dengan pengelola (*Acquirer*). Oleh karena POS ini tidak dapat diketahui keberadaannya atau lokasinya karena *merchant*nya sudah tutup, maka POS ini disebut dengan *Ghost / Phantom Terminal*.

c. *Skimming*

Yaitu suatu cara untuk memindahkan seluruh data yang ada di dalam *magnetic stripe* kartu kredit asli secara elektronik ke dalam *magnetic stripe* kartu kredit palsu. Alat untuk membaca dan memindahkan data dari kartu asli kepada kartu palsu tersebut disebut *Skimmer*.

B. Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Penyalahgunaan Kartu Kredit Menurut Hukum Positif Indonesia

Kebijakan hukum pidana dalam upaya penanggulangan kejahatan kartu kredit dilakukan dengan menggunakan 2 (dua) cara atau metode yaitu:

1. Upaya Penal dan
2. Upaya non penal.

Upaya penal untuk mengungkap kasus-kasus di bidang *carding* (kejahatan kartu kredit), dilakukan dengan menggunakan peraturan perundang-undangan antara lain adalah KUHP dan UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Langkah ini diambil karena belum ada undang-undang khusus yang mengatur tindak pidana yang berkaitan dengan

hal tersebut, kejahatan kartu kredit hanya diatur dalam pasal yang ada di dalam UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selanjutnya akan dibahas pasal-pasal yang digunakan untuk menjerat para pelaku sekaligus tersangka tindak pidana kejahatan kartu kredit (*carding*).

1. Penipuan

Dalam pasal 378 Kitab Undang-undang Hukum Pidana (KUHP), ditentukan bahwa : Barangsiapa dengan maksud untuk menguntungkan dirinya sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu, dengan tipu muslihat, ataupun rangkaian bohong, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun melepaskan piutang, diancam karena penipuan dengan penjara paling lama empat tahun.

2. Pemalsuan

Dalam ketentuan Pasal 263 KUHP ayat (1), ditegaskan bahwa : Barangsiapa yang membuat palsu atau memalsukan surat yang dapat menimbulkan suatu hak, perikatan atau pembebasan utang, atau yang diperuntukan sebagai bukti daripada sesuatu hal dengan maksud untuk memakai atau menyuruh orang lain memakai surat tersebut seolah-olah isinya benar dan tidak palsu, diancam jika pemakaian tersebut dapat menimbulkan kerugian, karena pemalsuan surat, dengan pidana penjara paling lama enam tahun. Sehubungan dengan hal tersebut, salah satu unsur yang paling esensial dari tindak pidana yang diatur dalam Pasal 263 KUHP, adalah : Adanya adanya surat palsu, kertas yang palsu atau yang dipalsukan. Untuk dapat menerapkan Pasal 263 KUHP pada tindak pidana kartu kredit, memang bahwa kartu kredit itu adalah jenis kertas walaupun plastik yang sudah dipalsukan oleh pelaku tindak pidana.

3. Pencurian

Dalam Pasal 362 Kitab Undang-undang Hukum Pidana (KUHP), ditentukan bahwa : Barangsiapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima

tahun atau pidana denda paling banyak sembilan ratus rupiah.

PENUTUP

A. Kesimpulan

1. Modus operandi kejahatan kartu kredit atau *carding* ada bermacam-macam yakni: *fraud application, non received card, lost/stollen card, altered card, totally counterfeiled, white plastic card, record of charge pumping, altered amount, telephon/mail ordered*, mengubah program *electronic data/draft capture dan fictius merchant*.
2. Kebijakan hukum pidana dalam upaya menanggulangi tindak pidana dengan menggunakan kartu kredit atau kejahatan kartu kredit atau *carding* dilakukan dengan menggunakan sarana penal yaitu penerapan Pasal 362, 378 dan 263 ayat (1) KUHP dan Pasal 32 ayat (1) UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan upaya non penal yaitu melakukan sosialisasi ke masyarakat tentang kejahatan kartu kredit dan dampaknya bagi pengguna kartu kredit. Selain itu juga dilakukan upaya penanggulangan *carding* secara preventif, dimana Kepolisian merekomendasikan kepada Bank Indonesia untuk melakukan pengawasan/pembatasan terhadap peredaran/penerbitan kartu kredit, menerbitkan buku merah tentang panduan pencegahan dan penanggulangan *carding* dan Bank Indonesia membentuk regulasi yang mengatur penggunaan kartu kredit sebagai pencegahan terjadinya *carding*. Untuk upaya penanggulangan secara represif, dilakukan upaya mediasi anatar pihak bank yang mengeluarkan kartu kredit, pemegang kartu kredit dan pelaku *carding* dengan mediator Bank Indonesia. Apabila tidak tercapai, pelaku diserahkan kepada Kepolisian untuk ditangani seperti kejahatan lainnya.

B. Saran

1. Dengan semakin majunya ilmu pengetahuan dan canggihnya teknologi, *modus operandi* yang ada sekarang masih bisa berkembang lagi, oleh

karenanya menjadi kewajiban dari aparat penegak hukum untuk mengantisipasi hal tersebut dengan lebih memperluas pengetahuan dibidang teknik informatika agar tidak ketinggalan pengetahuan dari para pelaku tindak pidana penyalahgunaan kartu kredit/*carding*.

2. Dalam rangka mencegah dan menanggulangi terjadinya kejahatan kartu kredit/*carding*, maka penerbit kartu kredit harus melengkapi kartu kredit yang diterbitkannya dengan *chip*, agar tidak dengan mudah terjadi pembobolan. Juga kepada hakim yang mengadili perkara kejahatan kartu kredit/*carding*, harus menjatuhkan hukuman yang maksimal agar pelaku kejahatan kartu kredit tidak akan mengulanginya lagi.

DAFTAR PUSTAKA

- Abdullah Mustafa; Ruben Achmad, *Intisari Hukum Pidana*, Ghalia Indonesia, Jakarta, 1983
- Hamzah Andi, *Asas-asas Hukum Pidana*, Rineka Cipta, Jakarta, 1991
- Halim A. Halim, *Hukum Pidana Dalam Tanya Jawab*, Ghalia Indonesia, Jakarta, 1986
- Indradi Ade Ary Syam, *Carding: Modus Operandi, Penyidikan Dan Penindakan*, Grafika Indah, Jakarta, 2006
- KUHAP dan KUHP*, Sinar Grafika, Jakarta, 2013
- Lamintang P.A.F, *Delik-Delik Khusus Kejahatan-Kejahatan Terhadap Kepentingan Negara Hukum*, Sinar Baru, Bandung, 1987
- Lemaire W.L.G, *Dasar-Dasar Hukum Pidana Indonesia*, Terj. P.A.F.Lamintang, PT Citra Aditya Bakti, Bandung, 1997.
- Moeljatno, *Azas-Azas Hukum Pidana*, Bina Aksara, Jakarta, 1983.
- Markas Besar Kepolisian Negara Republik Indonesia, *Buku Petunjuk Tentang Penyidikan Tindak Pidana Yang Berhubungan Dengan Kartu Kredit*, 1998
- Panjaitan Leo.T, *Analisis Penanganan Carding dan Perlindungan Nasabah Dalam UU ITE*, Jurnal, Jakarta, 2012
- Poernomo, Bambang, *Azas-Azas Hukum Pidana*, Ghalin Indonesia, Cetakan ke-3, 1978.
- Rofikah, Supanto, Ismunarno, Sabar Slamet, *Model Penanggulangan Carding*, diakses

dari <https://jurnal.uns.ac.id> pada tanggal 6 Agustus 2019.

Suseno Sigid dan Syarif A Barmawi, *Kebijakan Pengaturan Carding Dalam Hukum Pidana Di Indonesia*, diakses dari jurnal.unpad.ac.id pada tanggal 7 Agustus 2019,

Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif*, Rajawali, Jakarta, 1985, Utrecht E, *Hukum Pidana I*, *Pustaka Tinta Masyarakat*, Surabaya, 1986