Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik no.11 Tahun 2008

Leo T. Panjaitan

Teknik Elektro, Universitas Mercu Buana, Jakarta

Abstrak

Teknologi Informasi dan Komunikasi (TIK) secara langsung dan tidak langsung berpotensi melahirkan kejahatan-kejahatan siber (Cybercrime) khususnya Carding. UU ITE No.11 tahun 2008 merupakan jaminan kepastian hukum yang akan membuat seluruh aktivitas pemanfaatan TIK di dalam negeri terlindungi dengan baik dari potensi kejahatan dan penyalahgunaan teknologi. Kepastian hukum ini juga harus dirasakan oleh pelaku industri kartu kredit termasuk kastemer. Dengan cara ini maka bertransaksi di internet dengan menggunakan kartu kredit sebagai alat pembayaran dapat berlangsung secara aman dan nyaman.

Metode yang digunakan dalam penelitian ini adalah yuridis normatif dengan tambahan analisa data statistik untuk mengkaji penanganan carding di Bank X. Pada prakteknya UU ITE No.11 tahun 2008 dapat menjadi landasan penegakan hukum yang baru di bidang kartu kredit yang pemakaiannya dalam bidang pembayaran sudah semakin meluas terutama pada perdagangan elektronik (e-commerce). Untuk itu perlu segera diupayakan sosialisasi UU ITE No.11 tahun 2008 ke seluruh pemangku kepentingan untuk melindungi industri kartu kredit dari kejahatan kerah putih.

***Kata kunci**:* Perlindungan Hukum Nasabah Bank, Kejahatan Dunia Maya, Carding, Kebijakan Carding, Cybercrime

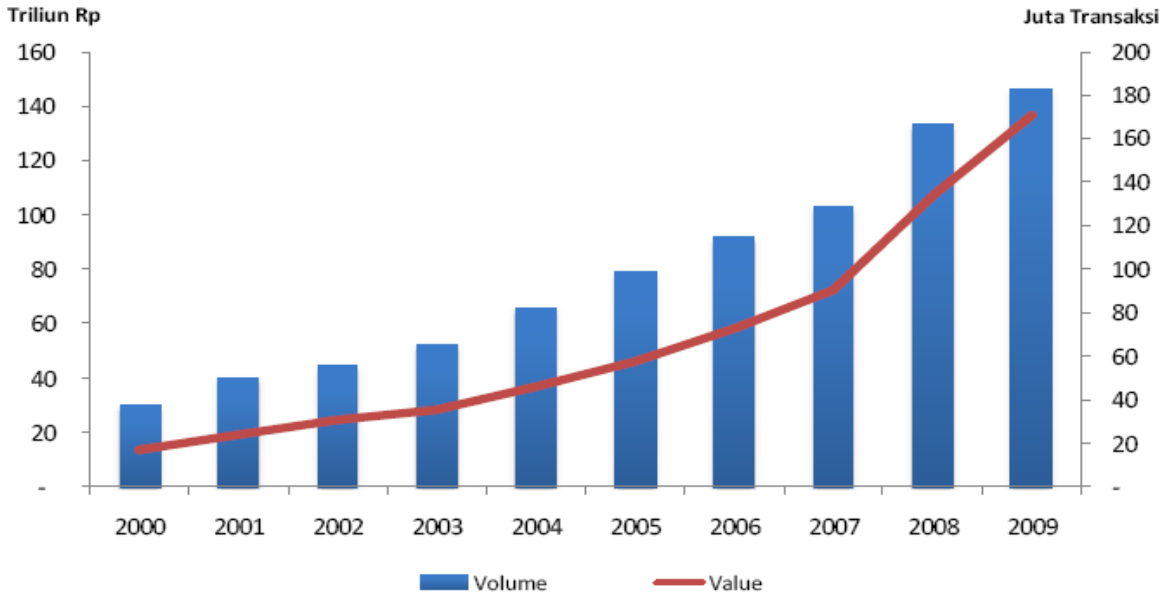
1. LATAR BELAKANG

Kartu kredit merupakan alat pembayaran yang semakin populer di masyarakat dunia bahkan Indonesia. Kartu kredit sebagai alat bayar merupakan jenis APMK yang keberadaannya paling lama digunakan di negeri ini sejak era 1980-an. Pada awalnya, pemegang kartu kredit masih terbatas pada kelompok-kelompok sosial tertentu dan penggunaannya ditujukan untuk pembayaran yang bersifat khusus. Perkembangan tersebut sebenarnya didorong oleh berbagai faktor yang berkenaan dengan pengunaan kemudahan, kepraktisan dan citra diri pemegang kartu

(Abdulkadir Muhammad dan Rilda Murniati, 2000).

Saat ini dengan perkembangan kebutuhan alat bayar yang lebih efisien, mudah dan nyaman digunakan, alat bayar melalui kartu kredit ini menjadi salah satu primadona di masyarakat. Berdasarkan Laporan Sistem Pembayaran dan Pengedaran Uang Bank Indonesia (LSPPU BI) tahun 2009 jumlah pemegang kartu kredit di Indonesia sudah mencapai lebih dari 12 juta kartu yang beredar dari total 20 penerbit (issuer) di Indonesia.

Perkembangan jumlah pemegang kartu kredit selama kurun waktu 10 tahun terakhir di Indonesia menunjukkan tren yang meningkat seiring dengan kemajuan industri perbankan. Selama lima tahun terakhir rata-rata pertumbuhan per tahun sebesar 18%. Naiknya tren jumlah kartu selama kurun waktu tersebut turut mendorong peningkatan penggunaannya. Di sisi nilai pertumbuhan per tahun mencapai 30%, sementara itu di sisi volume mencapai 19%. Hal ini terlihat dari Gambar 1 (LSPPU BI, 2009) di bawah ini:



Gambar 1 Jumlah Nilai dan Volume Transaksi Kartu Kredit di Indonesia

Jumlah nilai transaksi kartu kredit di tahun 2009 mencapai Rp. 136,7 triliun dan volume mencapai 182,6 juta transaksi. Apabila dibandingkan dengan tahun 2008, nilai transaksi meningkat 27% dan volume meningkat 10%.

Sejak berkecimpung di industri kartu kredit tahun 1997, perkembangan jumlah pemegang kartu Bank X begitu pesat dan telah menjadi salah satu *profit center* dalam *business unit* yang ada di lingkungannya. Data Bank X (*Business Presentation, Card Center* Bank X, 2009) sebagai berikut:

Tabel 1 Posisi Kartu Kredit Bank X di Indonesia Tahun 2009

Keterangan	Matrix	Bank X	Industri	Market Share (%)	Rank
CIF (Card in Force)	(000)	1,339	12,084	11,10%	4
ENR (Outstanding Balance)	(IDR Billion)	2,688	34,709	7,70%	5
Sales Volume - Issuing	(IDR Billion)	6,072	98,8	6,10%	6

Oleh karena itu, bisnis kartu kredit menjadi salah satu mesin profit setiap bank dan lembaga bukan bank baik dalam meraih kastemer baru maupun mencetak portofolio bisnis secara variatif. Namun praktek industri kartu kredit di Indonesia belum sepenuhnya aman dari tangan-tangan jahil atau pelaku kejahatan kartu kredit. Carding adalah bentuk *cyber crime* yang masih menjadi modus operandi para pelaku atau fraudster. Pada Januari 2004, Indonesia pernah dinobatkan sebagai negara nomor 1 dalam *top countries by percentage of fraudulent transaction* dan negara nomor 3 dalam *top countries by total volume of fraudulent transaction* dalam penelitian tentang keamanan internet di dunia (Verisign Report, 2004).

Di lain pihak, Indonesia saat ini sudah memiliki suatu rezim hukum baru yang dikenal dengan hukum siber (Penjelasan Atas UU ITE) atau hukum telematika, yakni UU ITE (Informasi dan Transaksi Elektronik) No.11 tahun 2008. UU ITE lahir dari tuntutan global tentang perlunya negara-negara memiliki hukum siber atau *cyber law*, yang secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi.

Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik. Carding sendiri merupakan bagian *cyber crime* dalam transaksi perbankan yang menggunakan sarana internet sebagai basis transaksi khususnya sistem layanan perbankan *online* (*online banking*). Terjadinya carding oleh pelaku (*carder*) dengan cara memperoleh data kartu kredit secara tidak sah dengan memanfaatkan teknologi informasi (Internet) yaitu menggunakan nomor kartu kredit orang lain untuk melakukan pemesanan barang secara *online*. Komunikasi awalnya dibangun melalui *e-mail* untuk menanyakan kondisi barang dan melakukan transaksi. Setelah terjadi kesepakatan, pelaku memberikan nomor kartu kreditnya dan penjual mengirimkan barangnya.

Carding sendiri merupakan tindakan pidana yang bersifat *illegal interception*,[1] dan kemudian menggunakan nomor kartu kredit tanpa kehadiran fisik kartunya untuk belanja di toko *online* (*forgery*). Modus ini dapat terjadi akibat lemahnya sistem otentikasi yang digunakan dalam memastikan identitas pemesanan barang di toko *online*. Mengingat tindak pidana carding ini menggunakan sarana komputer dan atau jaringan komputer maka dapat menjadi salah satu jenis kejahatan yang dapat dimasukkan dalam legislasi kejahatan dunia maya (cyber crime law) menurut ITU (*ITU ToolKit for Cybercrime Legislation, Draft Rev*.February, 2010), sebagai berikut:

Barangsiapa dengan sengaja dan tanpa otorisasi sesuai dengan aturan prosedur pidana dan hukum lainnya di negara ini, memotong, dengan cara teknis, transmisi data komputer non-publik, isi data, atau data lalu lintas, termasuk emisi elektromagnetik atau sinyal-sinyal dari komputer, sistem komputer, atau jaringan yang membawa atau memancarkan sinyal-sinyal dimaksud, ke atau dari sebuah

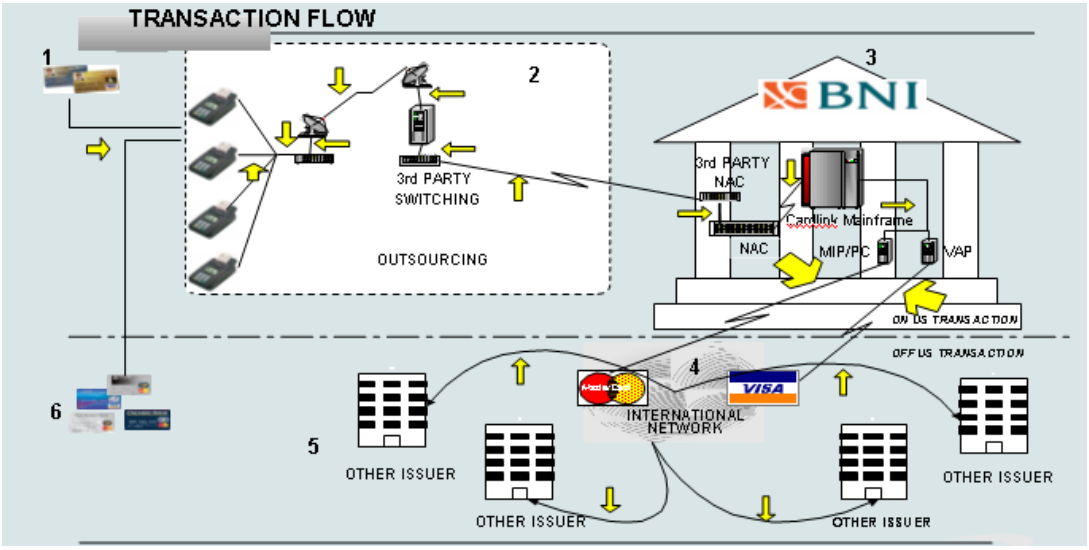
[1] Beberapa contoh dari *Illegal Interception* yaitu antara lain: penggunaan kartu asli yang tidak diterima oleh pemegang kartu sesungguhnya (*non received card*), kartu asli hasil curian/ temuan (*lost/ stolen card*), kartu asli yang dirubah datanya (*altered card*), kartu kredit palsu (*totally counterfeit*), penggandaan *sales draft* oleh oknum pedagang kemudian diserahkan kepada oknum *merchant* lainnya untuk diisi dengan transaksi fiktif (*record of charge pumping* atau *multiple imprint*), dan lain-lain.

komputer, sistem komputer dan / atau sistem yang terkoneksi, atau jaringan maka dianggap telah telah melakukan suatu pelanggaran pidana dengan jumlah denda sebesar_____ dan / atau penjara selama _____.

Faktor perlindungan nasabah bank atas terjadinya carding dikarenakan semakin berkembangnya layanan jasa *e-commerce* di Indonesia sekarang ini. Dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik dapat menjamin kepastian hukum di bidang *e-commerce*. Belanja on-line kini bukan lagi istilah yang asing bagi masyarakat Indonesia khususnya yang tinggal di wilayah perkotaan. Hal tersebut disebabkan semakin banyaknya issuer kartu kredit dari kalangan perbankan yang mengembangkan *internet payment gateway* (IPG) sebagai suatu bisnis yang mendatangkan keuntungan. Di masa mendatang, layanan e-commerce tampaknya akan menjadi sebuah tren yang meningkat seiring dengan kemajuan dunia telekomunikasi.

2. PERMASALAHAN

Untuk melihat gambaran transaksi kartu kredit dalam suatu bank maka dapat disampaikan Gambar 2 (Bank X, *EDC dan Network* , 2009) sebagai berikut:



Gambar 2 Alur Transaksi Kartu Kredit di Suatu Bank

Gambar 2 menjelaskan proses singkat alur transaksi sebagai berikut (sesuai nomor):

1. Nasabah melakukan transaksi di merchant (toko). Lalu kartu kredit digosok atau dicolok di mesin EDC. Data berisi informasi: nomor kartu kredit, *expiry date*, nama nasabah, CVC (*Card Verification Code*), *Credit limit*.
2. Data nasabah kemudian mengalir ke jaringan (network) LAN yang dikelola oleh pihak ketiga, dalam hal ini vendor atau perusahaan switching (outsourcing).
3. Aliran data kemudian masuk ke pusat data (data center) Bank X. Dari sini data kemudian diolah di dalam NAC (Network Access Control), Cardlink

Mainframe dan MIP (Mastercard Interface Processor) /VAP (Visa Access Point).

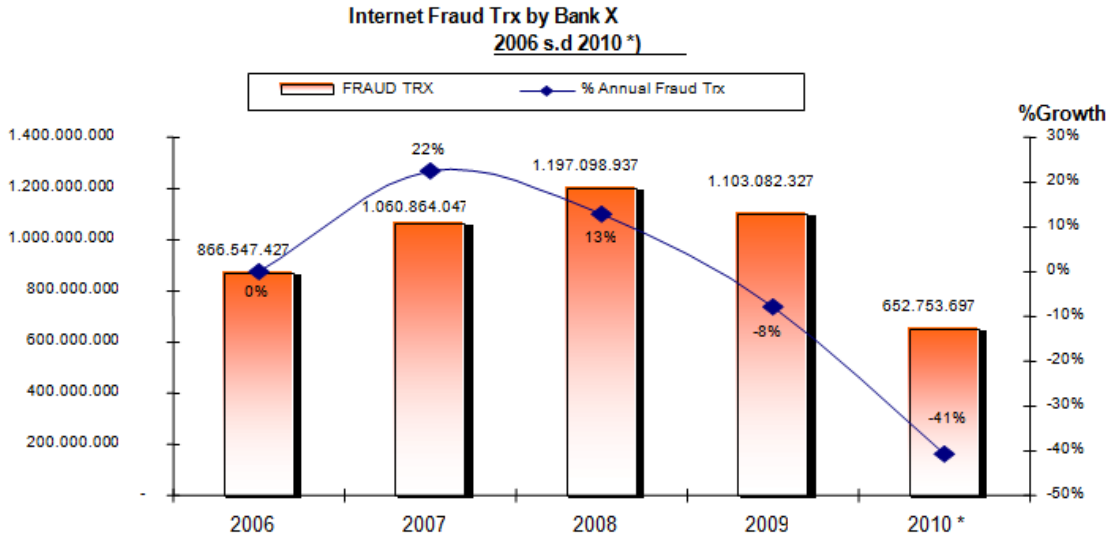
4. Setelah selesai data nasabah kemudian masuk ke network Visa/Master melalui gateway international.
5. Dari jaringan Visa/Mastercard ini, data nasabah akan dipilah berdasarkan issuernya, apakah kartu tersebut kartu kredit Bank X, Citibank, Mandiri dan sebagainya.
6. Kemudian proses data berulang (looping) dan apabila data nasabah valid dan outstanding kredit lancar atau mencukupi maka transaksi akan langsung di*approved* oleh mesin EDC. Nasabah membawa pulang barang belanjaannya.

Dari Gambar 2 dapat memunculkan titik kritis terjadinya risiko kejahatan kartu kredit yakni pada poin 2 ketika data nasabah masuk ke LAN perusahaan switching. Terjadinya tindak kejahatan dapat dimulai pada poin 2 yang mana pelaku melakukan *illegal interception* (intersepsi ilegal) dengan menyadap data nasabah kartu kredit secara lengkap. Data nasabah yang lengkap itu kemudian dilakukan *reprint* baik menggunakan teknik *skimming* maupun langsung belanja on-line di internet. Dari titik inilah sebenarnya proses carding itu kemudian mencuat. Artinya carder mendapatkan data kartu kredit yang valid melalui hasil curian.

Pada tanggal 13 Februari 2009, Mabes Polri berhasil menangkap tersangka Andre Christian Brail (Usia 28 thn) dan Khayrunisa (Usia 44 thn) yang diketahui telah melakukan kejahatan ini sejak tahun 2000. Modus kejahatan carding ini dengan memanfaatkan PIN dan nomor kartu kredit nasabah yang masih bisa digunakan untuk otorisasi secara ilegal. Selanjutnya, dengan menggunakan kartu kredit kosong dicetak melalui perangkat komputer dan mesin cetak canggih. Setelah itu kartu kredit bisa digunakan untuk transaksi seperti belanja di merchant (toko), menginap di hotel serta melakukan transaksi tarik tunai. Dari tangan para carder itu, Polisi berhasil mengumpulkan berbagai barang bukti yakni, 27 lembar kartu kredit palsu, delapan buah ponsel, sebuah mesin cetak embosser, sebuah skimmer merek MSR 2006, dua buah laptop, sebuah alat pembaca (umron) dan sebuah hard disk.

Sementara itu, tak kalah gaungnya kasus carding berikutnya yang muncul adalah yang dilakukan oleh seorang karyawan starbucks di MT Haryono, Tebet, Jaksel (Tempointeraktif.com, 19 Juli 2010). Penggelapan data nasabah dilakukan sekitar Maret hingga Juni 2010 dan terbongkar setelah lebih dari 41 nasabah melaporkan adanya transaksi ilegal pada kartu kreditnya. Modus operandi yang digunakan pelaku adalah dengan melakukan reprint (cetak ulang) struk transaksi dan kemudian mencatat kode verifikasinya (CVC). Dari situ sang carder berhasil menguasai ratusan data kartu kredit. Data kartu kredit selanjutnya digunakan untuk membayar transaksi pembelian alat elektronik Ipod Nano dan Ipod Touch secara online di Apple Online Store Singapura hingga lebih dari 50 kali.

Berdasarkan data Bank X, kejahatan carding masih dari tahun ke tahun masih kerap terjadi. Hal ini terlihat di gambar 3.



Gambar 3 Nilai Transaksi Carding yang Fraud melalui Internet – Bank X

Data di atas menggambarkan dari transaksi carding atau transaksi yang *fraud* (palsu) masih tetap terjadi meskipun dengan tren yang mulai menurun. Pertumbuhan transaksi fraud atau carding ini mengalami puncaknya pada tahun 2008 sebesar 13% (Rp.1,197 Miliar), lalu menurun sebesar 8% (Rp. 1,103 Miliar) di tahun 2009 dan menurun kembali di tahun 2010 sebesar 41% (Rp.653 Juta). Di lain pihak, di era ICT (Information and Communication Technology) transaksi on-line atau belanja internet tetap menjadi salah satu transaksi yang paling digemari oleh para nasabah.

Meskipun terjadi penurunan transaksi fraud seperti tampak pada Gambar 1.4 di atas namun bukan berarti transaksi belanja on-line di internet bebas dari segala tindak kejahatan. Perlindungan hukum baik kepada pihak perbankan dan nasabah harus menjadi perhatian semua pihak khususnya aparat penegak hukum dan legislator baik di Parlemen maupun Pemerintah. Keberadaan UU ITE No.11 tahun 2008 merupakan terobosan hukum yang luar biasa namun UU ITE belum secara eksplisit mengakomodasi transaksi perbankan melalui internet dengan menggunakan kartu (kredit dan debit) dan dampak-dampak yang berkaitan dengan kejahatan dunia maya (*cyber crime*). Oleh karena itu dalam kapasitasnya, UU ITE No.11 Tahun 2008 layak disebut sebagai undang-undang semi *cyber crime*.

3. KARTU KREDIT SEBAGAI ALAT PEMBAYARAN MENGGUNAKAN KARTU (APMK)

Keberhasilan pembangunan nasional di Indonesia sangat berdampak terhadap perbaikan tingkat kesejahteraan sosial dan ekonomi masyarakat yang didukung dengan perkembangan sarana dan prasarana transportasi, telekomunikasi, dan perkembangan *teknologi (high technology*). Hal ini dapat mendorong perkembangan dan potensi bisnis ritel yang semakin menarik dan menciptakan peluang bisnis bagi bisnis perbankan dalam mengembangkan dan memperkuat posisi bisnis *retail banking.* Bisnis ritel ini juga bertujuan untuk melakukan penyebaran resiko dan meningkatkan kontribusi laba perusahaan sebagai *profit center*.

Permintaan dan tuntutan nasabah terhadap kualitas produk dan jasa layanan perbankan juga telah semakin kompleks dan bervariasi. Perilaku nasabah *retail* telah semakin *bank minded*, sensitif, dan rasional dalam memilih produk, pelayanan, dan bank yang berkualitas. Hal ini menuntut dunia perbankan agar tanggap dan adaptif dalam mengantisipasi perkembangan selera pasar tersebut. Seiring itu permintaan terhadap produk kartu dan jasa layanan perbankan berbasis teknologi canggih lain seperti *Debit Card* (ATM) dan *Credit Card* juga semakin meningkat. Karena itu salah satu strategi pengembangan usaha yang dilakukan perbankan di era teknologi canggih saat ini adalah menjaring prospek bisnis ritel melalui sektor bisnis kartu yang mencakup kartu kredit.

Berbagai upaya tersebut bertujuan memperluas pasar dengan sasaran akhir meningkatkan profit, yang biasanya diperoleh penerbit apabila terdapat pengalihan kewajiban pembayaran menjadi kredit. Pengalihan kewajiban ini dikenal dengan istilah *revolving costumer*. Rata-rata industri kartu kredit di Indonesia mengenakan bunga bagi kewajiban nasabah tersebut sekitar 3,5%, bahkan untuk penarikan tunai bisa mencapai 4%, atau kalau kita hitung dalam setahun bunga tersebut dapat mencapai 42% untuk bunga pembayaran kewajiban pembelian dan 48% untuk penarikan tunai. Jumlah tersebut jika dibandingkan dengan bunga bank untuk kredit tanpa agunan nilainya bisa mencapai lebih dari 3 kali lipat.

4. PENGATURAN KARTU KREDIT

Kartu kredit adalah alat bayar yang tidak memiliki jaminan (*unsecured loan*) yang diberikan oleh bank penerbit kepada nasabah bank karena kredibilitas yang bersangkutan. Pengaturan kartu kredit mengacu pada ketentuan Bank Indonesia dan juga kebijakan masing-masing bank (*self-regulatory bank*). Oleh karena itu dalam prakteknya bank akan memberikan pengaturan yang menyangkut pedoman kerja bagi semua pejabat yang berwenang terhadap perkreditan dalam mengelola bisnis, sehingga tercapai keseimbangan antara kuantitas dan kualitas dalam portofolio dan risiko kredit. Selain itu seorang karyawan bank yang terlibat dalam aktivitas perkreditan harus mengetahui ketentuan dan peraturan eksternal yang berkaitan dengan bisnis yang dijalankan seperti peraturan pemerintah, ketentuan Bank Indonesia, serta peraturan dari MasterCard International dan Visa International.

Mengingat perkembangan kartu kredit masih terbilang relatif baru dibandingkan dengan alat bayar lainnya, seperti uang tunai, cek dan sebagainya, maka tentang berlakunya kartu kredit tidak diketemukan dasar hukumnya yang tegas dalam Kitab Undang-Undang. Karenanya baik KUH Dagang maupun KUH Perdata tidak menyebut-nyebut istilah Kartu kredit.

Beberapa peraturan yang sifatnya untuk memenuhi kebutuhan bagi kelancaran atau kemudahan dalam lalu lintas pembayaran yaitu:

a. Keputusan Presiden Republik Indonesia Nomor 61 Tahun 1988, tentang Lembaga Pembiayaan.
b. Keputusan Menteri Keuangan Republik Indonesia Nomor 1251/KMK.013/1998 tentang Ketentuan dan tata cara Pelaksanaan Lembaga Pembiayaan.

c. Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.
d. Peraturan Bank Indonesia (PBI) Nomor: 7/52/PBI/2005 dan PBI Nomor: 11/11/PBI/2009 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu.

Sebagai pelaksanaan dari Undang-Undang No. 23 Tahun 1999 tentang Bank Indonesia sebagaimana telah diubah dengan Undang-Undang No. 3 Tahun 2004, khususnya terkait dengan tugas Bank Indonesia dalam mengatur dan menjaga kelancaran sistem pembayaran, Bank Indonesia berwenang antara lain melaksanakan dan memberikan persetujuan dan izin atas penyelenggaraan jasa sistem pembayaran dan mewajibkan penyelenggara jasa sistem pembayaran untuk menyampaikan laporan tentang kegiatannya.

5. PENGATURAN KARTU KREDIT

Dalam pembahasan di bagian 1, Carding adalah transaksi *fraud* (penyimpangan) yang mana si pelaku (*fraudster*) tidak harus memegang fisik kartu kredit. Si Pelaku hanya memerlukan nomor kartu kredit dan beberapa informasi seperti *expiry date* dan *CVC (Card Verification Code).* Dalam industri kartu kredit, pihak bank penerbit mengenal carding sebagai tindakan *Card Not Present* (CNP) yang bisa berakibat pada penyimpangan (fraud) transaksi baik yang terjadi secara *on-line* dalam *e-commerce* maupun transaksi ritel *off line*.

Oleh karena itu perlu disampaikan Kebijakan Carding dan Penanganannya di Bank X yang termaktub dalam *electronik commerce transactions* (SOP Bank X, 2009) sebagai berikut:

1. *Electronic Commerce Transaction*
   Transaksi jual beli barang/jasa melalui media komunikasi elektronik atau yang dikenal dengan internet, dimana tidak terjadi pertemuan secara langsung antara penjual (merchant) dengan pembeli (pemegang kartu).
2. Transaksi kartu kredit ada 2 (dua) jenis, yaitu:
   a. *Card Present Transaction*, yakni transaksi kartu kredit secara langsung (*face to face transaction*).
   b. *Card-Absent (Non-Present) Transaction*, yakni transaksi kartu kredit secara tidak langsung (tanpa keberadaan Pemegang kartu dan fisik kartu kredit).
3. Dalam *card-absent transaction* terdapat beberapa macam transaksi, antara lain sebagai berikut:
   a. Electronic Commerce Transactions.
   b. Mail/Phone Order Transactions.
   c. Recurring Transactions.
   d. Telephone Service Transactions.
4. Dalam akseptasi merchant e-commerce perlu disampaikan hal-hal sebagai berikut:
   a. Akuisisi dan Pemeliharaan Merchant
   b. Operasional Merchant.
   c. Minimalisasi Fraud.
   d. Penanganan Dispute Transaction

5. Operasional Merchant e-commerce
   a. Merchant wajib mendapatkan sertifikasi Verified By Visa (VBV) serta MasterCard Secure Code (MSC).
   b. Merchant Wajib mengimplementasikan pengamanan dan pencegahan terhadap fraud, antara lain dengan menyediakan:
      1) IP Check up
      2) Geo Locator
      3) Address verification
      4) Pengamanan yang dituangkan dalam Perjanjian Kerjasama antara Bank X dengan merchant.

6. SIFAT PENELITIAN

Penelitian ini bersifat deskriptif analitis. Tujuan penelitian deskriptif adalah menggambarkan secara tepat, sifat individu, suatu gejala, keadaan atau kelompok tertentu (Koentjaraningrat, 1997). Deskriptif analitis berarti bahwa penelitian ini menggambarkan suatu peraturan hukum dalam konteks teori-teori hukum dan pelaksanaannya, serta menganalisis fakta secara cermat tentang penggunaan peraturan perundang-undangan dalam analisis penanganan carding dan perlindungan nasabah dalam kaitannya dengan UU ITE No.11 tahun 2008.

Data yang diperoleh melalui penelitian kepustakaan, adalah data sekunder, yang meliputi bahan hukum primer, sekunder dan tersier:

1) Bahan hukum primer (bahan hukum primer merupakan bahan hukum yang bersifat otoritatif, artinya mempunyai otoritas), terdiri dari:
   a. Undang-undang Informasi dan Transaksi Elektronik (ITE) No.11 tahun 2008.
   a. Undang-undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-undang Nomor 7 Tahun 1992 tentang Perbankan.
   b. Kitab Undang-undang Hukum Pidana.
   c. Peraturan Bank Indonesia Nomor: 11/11/PBI/2009 Tentang Penyelenggaran Kegiatan Alat Pembayaran Menggunakan Kartu.
2) Bahan hukum sekunder (berupa semua publikasi tentang hukum yang bukan merupakan dokumen-dokumen resmi), terdiri dari:
   a. MasterCard International Guide and Policy.
   b. Hasil-hasil penelitian mengenai Kartu Kredit.
3) Bahan hukum tersier (berupa bahan hukum penunjang yang memberi petunjuk dan penjelasan terhadap bahan hukum sekunder), terdiri dari:
   a. Kamus Hukum.
   b. Ensiklopedia Hukum.
   c. SOP Kartu Kredit, Bank X.

Subyek penelitian adalah transaksi pemegang kartu kredit dari PT. Bank X, Tbk yang mengalami fraud dalam kasus carding. Selanjutnya metode pengumpulan data yang dipakai adalah dengan cara *non random*, yaitu *purposive sampling*. Metode ini dipakai, karena data yang diperoleh akan memberikan arah pada

kesimpulan penelitian. Untuk itu, peneliti menetapkan syarat-syarat tertentu di dalam memilih *sample,* yaitu pihak-pihak yang terlibat ataupun mengetahui adanya praktek penggunaan Kartu Kredit.

7. DEFINISI OPERASIONAL

Adapun yang menjadi batasan dari definisi operasional yang akan dipergunakan dalam penelitian ini adalah sebagai berikut:

1. *Issuer* atau Penerbit adalah Bank atau Lembaga Selain Bank yang menerbitkan Alat Pembayaran Dengan Menggunakan Kartu untuk Pemegang Kartu dengan menggunakan merek tertentu atas persetujuan Prinsipal. (Pasal 1 ayat 13, PBI No. 7/52/PBI/2005 Tentang Penyelenggaraan Kegiatan APMK).
2. *Acquirer* adalah Bank atau Lembaga Selain Bank yang melakukan kegiatan Alat Pembayaran Dengan Menggunakan Kartu yang dapat berupa *financial acquirer* dan/atau *technical acquirer*. (Pasal 1 ayat 14, PBI No. 7/52/PBI/2005 Tentang Penyelenggaraan Kegiatan APMK).
3. *Financial Acquirer* adalah *Acquirer* yang melakukan pembayaran terlebih dahulu atas transaksi yang dilakukan oleh Pemegang Kartu. (Pasal 1 ayat 15, PBI No. 7/52/PBI/2005 Tentang Penyelenggaraan Kegiatan APMK).
4. *Technical Acquirer* adalah *Acquirer* yang menyediakan sarana yang diperlukan dalam pemrosesan Alat Pembayaran Dengan Menggunakan Kartu. (Pasal 1 ayat 16, PBI No. 7/52/PBI/2005 Tentang Penyelenggaraan Kegiatan APMK).

Carding atau disebut *Card Not Present Transaction* adalah bentuk kejahatan menggunakan nomor kartu kredit orang lain untuk dibelanjakan (*non face to face transaction*) tanpa sepengetahuan pemiliknya yang sah. Transaksi lazimnya dilakukan secara elektronik.

8. HIPOTESA

Penelitian ini bersifat yuridis normatif untuk meneliti berbagai undang-undang yang berhubungan dengan tindakan cybercrime dan carding serta peraturan terkait lainnya yang menjadi ketentuan di Bank X. Penelitian hukum yang berbasis yuridis normatif tidak memerlukan uji hipotesis sebagaimana layaknya penelitian soisal (Peter Mahmud Marzuki, 2005). Namun mengingat penelitian ini mengambil studi kasus pada pengelolaan carding di Bank X maka diperlukan hipotesa dengan maksud untuk mendukung data penelitian khususnya yang berkaitan dengan penanganan carding di Bank X. Hipotesa atau asumsi dimaksudkan sbb:

1. Akan mendapatkan pemahaman yang mendalam mengenai bentuk *cyber crime* di bidang perbankan dan perlindungan nasabah dalam kasus carding yang dikaitkan dalam UU ITE No.11 tahun 2008?
2. Akan menguraikan dan menjelaskan tentang pencegahan dan penanganan kasus carding yang dilakukan oleh Bank X.

9. JENIS-JENIS FRAUD YANG TERJADI DALAM APMK (ALAT PEMBAYARAN MENGGUNAKAN KARTU)

Fraudster juga tidak pernah kehabisan akal untuk mencari celah. Ketika para penyelenggara mulai meningkatkan fitur keamanan kartu dari kemungkinan timbulnya kejahatan, para fraudster pun mengambil celah melalui kegiatan transaksi berbasis elektronik yang menggunakan email maupun website untuk berbelanja online yang kerap mengharuskan para pemegang kartu untuk memberikan identitas mereka. Pada gilirannya pencurian identitas pada transaksi online meningkat. Dan ketika para penyelenggara memfokuskan pada peningkatan keamanan untuk berbelanja online, maka fraud pada proses penyampaian kartu dan aktivasinya meningkat.

Untuk itu dalam industri kartu kredit terdapat kategori-kategori fraud yang baik yang dilakukan pada transaksi *face to face* (fisik) maupun fraud dalam transaksi on line (*Non Face to Face*) (LSPPU BI, 2009) diantaranya sebagai berikut:

1. *Lost and Stolen Cards*. Setelah dicuri, biasanya fraudster memakai kartu (biasanya kartu kredit atau kartu debet) untuk melakukan pembelanjaan dengan nilai yang relative kecil tapi sering.
2. *Fraudulent Applications (FA)*. Jenis fraud yang dilakukan fraudster yang berpura-pura sebagai calon pemegang kartu dengan cara memberikan data-data identitas palsu pada saat pengisian formulir pengajuan kartu baik itu kartu kredit, ATM, dan Debet.
3. *Account Takeover*. Fraud jenis ini dilakukan oleh fraudster dengan cara mengubah identitas pemilik kartu seperti alamat yang terdaftar pada kartu yang telah ada sebelumnya.
4. *Unauthorized Use of Account Numbers (CARDING)*. Hampir sama dengan jenis fraud yang sudah-sudah. Fraudster menggunakan kartu yang bukan miliknya untuk melakukan pembelanjaan melalui mekanisme transaksi yang tidak membutuhkan keberadaaan kartu (card not present) dan transaksi bersifat online.
5. *Counterfeit Cards and Skimming*. Jenis fraud yang paling banyak terjadi dan mekanismenya lebih canggih dibandingkan dengan fraud jenis lain. Fraud jenis ini biasanya terjadi pada kartu yang masih menggunakan *magnetic stripe* sebagai media penyimpan data.
6. *Not Received Items (NRI)*. Apakah Anda pernah mengajukan permohonan untuk memiliki kartu kredit tapi kartu tersebut tidak pernah sampai ke tangan Anda? Bisa saja kartu atas nama Anda telah di-fraud. Fraud yang mungkin terjadi dan dikenal dengan istilah *Not Received Items* (NRI). Fraudster bisa saja adalah orang dalam maupun orang luar yang mendapatkan informasi mengenai pengiriman kartu.
7. *Phising*. Seiring kemajuan teknologi, memungkinkan adanya metamorfosa bentuk fraud. Akhir-akhir ini banyak fraudster menggemari mekanisme fraud yang satu ini. Selain tidak perlu susah payah beranjak dari depan layar komputer memantau perkembangan jumlah account yang sudah berhasil didapat, fraud jenis ini membutuhkan software perekam data yang mulai marak diperjualbelikan di pasar gelap.

Di Indonesia regulasi mengenai kartu kredit semakin ditingkatkan dari tahun ke tahun oleh Bank Indonesia. Migrasi kartu magnetic stripe (kartu digesek) telah dilakukan oleh seluruh issuer ke kartu berbasis chip atau yang dikenal sebagai kartu EMV (*European Master Visa Payment System*). Per 01 Januari 2009 seluruh issuer kartu kredit di Indonesia telah sukses melakukan compliance (kepatuhan) regulasi BI. Pemakaian kartu EMV ini dapat meminimalisir risiko fraud karena kartu chip ini cukup terlindungi dari tindakan *skimming* atau *counterfeit* yang dilakukan oleh penjahat cyber.

10. *CYBER CRIME* (KEJAHATAN DUNIA MAYA) YANG BERKAITAN DENGAN CARDING

Membahas masalah kejahatan dunia maya merupakan sesuatu yang menarik dan menantang namun sesungguhnya apakah yang dimaksud dengan cybercrime atau kejahatan dunia maya (internet) itu? Dalam beberapa literatur, *cyber crime* sering diidentikkan sebagai *computer crime*. *The U.S. Department of Justice* memberikan pengertian *computer crime* sebagai:"…*any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution*". Pengertian lainnya diberikan oleh *Organization for Economic Cooperation and Development (OECD)*, yaitu: "*any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*". Andi Hamzah dalam bukunya Aspek-aspek Pidana di Bidang Komputer (1989) mengartikan: "*kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal*".

Indonesia saat ini telah memiliki Undang-Undang Informasi dan Transaksi Elektronik No.11 tahun 2008 (UU ITE) yang menjadi payung hukum secara general (*lex generalis*) bagi penegakan hukum di bidang kejahatan dunia maya (*cyber crime law*). Carding sendiri merupakan tindak pidana kejahatan yang merupakan bagian dari cybercrime. Tindak pidana carding tidak dapat dipisahkan dari maraknya perkembangan ICT (Information and Communication Technology) saat ini dimana internet menjadi tulang punggung telekomunikasi dunia.

Berikut ini beberapa contoh tindak pidana yang terjadi di dunia maya (Agus Rahardjo, 1999):

1. Tindakan sengaja dan melawan hukum, dengan maksud untuk menguntungkan diri sendiri atau orang lain menggunakan nama domain yang bertentangan dengan hak-hak pemilih yang telah digunakan oleh seseorang merupakan tindak pidana.
2. Tindakan dengan sengaja dan melawan hukum mengakses data suatu bank yang memberikan layanan *internet banking* dengan menggunakan *password* milik orang lain secara tanpa hak dan diluar kewenangannya melalui komputer atau media lainnya dengan atau tanpa merusak sistem pengamanan.
3. Tindakan dengan sengaja atau melawan hukum dengan maksud untuk menguntungkan diri sendiri atau orang lain menggunakan kartu kredit atau alat pembayaran elektronik lainnya milik orang lain, atau menyalahgunakan PIN milik orang lain dalam transaksi elektronik.
4. Tindakan dengan sengaja atau melawan hukum secara tanpa hak mengakses, menyimpan, mengumpulkan atau menyerahkan kepada yang

> orang tidak berhak data nasabah (seperti PIN), data kartu kredit atau pembayaran elektronik lainnya secara tidak berwenang dalam suatu media komputer atau media lainnya dengan maksud untuk menguntungkan diri sendiri atau orang lain.

Dari penjelasan di atas maka sebenarnya kebocoran kartu kredit terjadi karena adanya *Data Leakage* (Al. Wisnubroto, 2010). Istilah *data leakage* awalnya dikemukakan oleh Yusuf Randy (Si Raja Komputer era 1980-an) dalam bukunya ”Proteksi Terhadap Kriminalitas Dalam bidang Komputer”. Data Leakage (Kebocoran Data) adalah suatu pembocoran data rahasia yang dilakukan dengan cara menulis data rahasia tersebut ke dalam kode-kode tertentu sehingga data tersebut dapat dibawa keluar tanpa diketahui oleh pihak yang bertanggungjawab.

Kasus carding di Indonesia bermunculan ketika terjadi *booming* internet di era tahun 2000-an. Beberapa kota seperti Jakarta, Bandung dan Yogyakarta menjadi pusat-pusat carder dalam melancarkan aksi pencurian data kartu kredit. Aksi-aksi cybercrime ini mengakibatkan pada tahun 2004, transaksi on-line yang berasal dari IP (Internet Protocol) Indonesia diblokir oleh dunia internasional. Dari kasus-kasus cybercrime khususnya carding tersebut yang benar-benar diproses di pengadilan di Indonesia dapat dihitung dengan jari. Sangat jarang muncul ke media massa para carder dijerat dengan hukum yang setimpal dengan perbuatannya.

Sementara itu kasus-kasus carding di Indonesia telah lama muncul dan telah diputuskan perkaranya oleh pengadilan. Dalam keputusan hakim, sebagian besar kasus tersebut dikenakan pasal-pasal dalam KUHP. Berikut adalah tabel 2 kasus card di Indonesia yang pernah masuk ke pengadilan sebagai berikut:

Tabel 2 Kasus-kasus Kejahatan Komputer dan Carding di Indonesia

No	Perkara	Salinan Putusan	Pasal Yang Dikenakan
1.	Putusan Pengadilan Jakarta Pusat tahun 1988 telah menerapkan pasal Pencurian dalam kasus ”Unauthorized Transfer” dana BNI 46 New York Agency	Salinan Putusan Pengadilan Negeri Jakarta Pusat No.135/X/Pid.B/1987/PN.Jkt.Pst tanggal 11 Maret 1988 a.n **Seno Adjie**	Pasal 363 KUHP: ayat 4 berbunyi: *Pencurian yang dilakukan oleh dua orang atau lebih dengan bersekutu*
2.	Putusan Pengadilan Jakarta Barat tahun 1989 telah menerapkan pasal pencurian dalam kasus ”Data Diddling” Bank Bali Cabang Jakarta Barat	Salinan Putusan Pengadilan Negeri Jakarta Barat No.1050/Pid.S/1989/PN.Jkt.Brt tanggal 20 November 1989 a.n **Budiman Hidayat**	Pasal 362 KUHP: *Barang siapa yang mengambil suatu barang, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk memilikinya secara melawan hukum diancam karena pencurian dengan pidana penjara maksimum lima tahun.*
3.	Putusan Pengadilan Negeri Sleman tahun 2002 telah menerapkan pasal tentang penipuan dalam kasus Carding	Salinan Putusan Pengadilan Negeri Sleman No.94/Pid.B/2002/PN.Slmn a.n **Petrus Pangkur alias Boni Diobokobok**	Pasal 378 KUHP: *Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain dengan melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupun dengan rangkaian kebohongan menggerakkan orang lain untuk*

			menyerahkan sesuatu benda kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun.
4.	Putusan Pengadilan Negeri Semarang tahun 2003 telah menerapkan pasal tentang pencurian dalam kasus Carding	Salinan Putusan Pengadilan Negeri Semarang No.504/Pid.B/2003/PN.Smg	Pasal 362 KUHP: *Barang siapa yang mengambil suatu barang, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk memilikinya secara melawan hukum diancam karena pencurian dengan pidana penjara maksimum lima tahun.*

Dari tabel 2 di atas nampak kasus-kasus carding yang masuk ke pengadilan dapat dihitung dengan jari. Apabila didalami lebih lanjut kasus carding itu hampir sama dengan tindak pidana pencurian aliran listrik secara ilegal yang dapat merugikan konsumen ataupun PLN sebagai provider. Selain itu kejahatan carding juga bersifat finansial dimana si pelaku dapat menjalankan transfer dana secara ilegal. Dengan demikian sangat tidak tepat kalau terjadi kasus carding pasca UU ITE ini, carder dijerat dengan tindak kriminal biasa yakni KUHP Pasal 362, 363 dan 378. Carder harus dijerat dengan UU ITE No.11 tahun 2008 dengan pasal-pasal yang berhubungan dengan *illegal interception, diantaranya* pasal 32.

Dalam hal fisik kartu kredit, sejak awal 2009 bank-bank penerbit telah melakukan migrasi kartu dari magnetic stripe ke EMV atau Chip Card. Perubahan fisik ini memang terbukti dapat mengurangi risiko fraud khususnya pemalsuan kartu kredit, atau yang dikenal dengan *counterfeit*. Namun pada awal tahun 2010 *Cambridge University* mengungkapkan temuan adanya celah keamanan kritikal pada CHIP dan PIN berbasis kartu EMV setelah melakukan serangkaian uji keamanan. Para peneliti di *Cambridge University* (IEEE Symposium on Security and Privacy, Journal, *"Protocol Failure"*, 2010) telah menemukan sebuah celah keamanan pada protokol EMV yang memiliki kemampuan berkomunikasi dengan semua terminal POS (Point of Sale) dan mesin-mesin ATM yang mengeksekusi otentikasi pembayaran kartu kredit dan debit. *Cambridge University* kemudian melancarkan "serangan" (*the man-in-the middle*) untuk memperdaya "Card reader" agar mengotentikasi sebuah transaksi sekalipun transaksi menggunakan PIN yang tidak valid. Pada tes berikutnya, tim Cambridge melakukan otentikasi berbagai transaksi tanpa menggunakan PIN yang valid dengan menggunakan Kartu Kredit yang diterbitkan oleh Barclaycard, Co-operative Bank, Halifax, Bank of Scotland, HSBC dan John Lewis.

Permasalahan utama adalah manipulasi pada protokol EMV menyebabkan kartu dan terminal menghasilkan data yang ambigu pada proses verifikasi, dimana Bank akan menerima verifikasi tersebut sebagai valid. Ini sebabnya terminal POS tetap merekam bahwa sebuah verifikasi PIN berlangsung sukses, sementara kartu menerima sebuah pesan verifikasi yang tak mengindikasikan bahwa PIN telah digunakan (oleh pihak lain). Otorisasi yang dikeluarkan oleh terminal selanjutnya diterima oleh Bank, dan transaksi pun berproses.

Pada intinya teknologi tidak dapat seratus persen menjamin bahwa transaksi kartu kredit secara on-line akan aman dari tangan-tangan jahil. Oleh karena itu,

hukum lah yang menjadi solusi melalui perlindungan kepada warga negara khususnya nasabah yang kemudian menjadi korban kejahatan elektronik. K. Daniel Wong (2005) menyatakan bahwa serangan *a man in the middle* terjadi ketika si penyerang (*attacker*) berada di tengah arus komunikasi dua pihak. Si penyerang bebas mendengarkan dan mengubah percakapan antara dua pihak. Jadi dengan serangan tipikal ini, si penyerang tidak hanya pasif mendengarkan tetapi juga aktif mengubah komunikasi yang terjadi. Sebagai contoh, pada percakapan antara Mora dan Zeni, Encep menjadi pihak yang ditengah melakukan *a man in the middle attack*. Encep tidak hanya bisa mendengarkan percakapan itu, namun juga bisa mengubah percakapannya. Ketika Mora berkata kepada Zeni, ”besok kuliah Pak Aloy dimulai jam 10”, Encep bisa mengubahnya menjadi “besok kuliah Pak Aloy dibatalkan”. Sehingga Zeni mengira kuliah yang dimulai jam 10 dengan dosen Pak Aloy tidak jadi berlangsung alias dibatalkan.

A Man in the Middle Attack bisa terjadi karena sebelum berkomunikasi kedua belah pihak tidak melakukan *authentication*. Otentikasi berguna untuk memastikan identitas pihak yang berkomunikasi, apakah saya sedang berbicara dengan orang yang benar, ataukah orang ketiga (*the person in the middle*)? Tanpa Otentikasi, Mora akan mengira sedang berbicara dengan Zeni, sedangkan Zeni juga mengira sedang berbicara dengan Mora. Padahal bisa jadi sebenarnya Mora sedang berbicara dengan Encep dan Zeni juga sedang berbicara dengan Encep. Dengan demikian Encep di sini bertindak sebagai *“the person in the middle”*.

11. MANAJEMEN PENANGANAN CARDING DI BANK X

Sejak tahun 2007, Bank X memiliki unit khusus yang bernama *”Early Detection Unit”* yang bertugas untuk memantau, menganalisis dan mencegah sedini mungkin transaksi-transaksi kartu kredit yang berpotensi fraud baik yang digunakan di internet secara *on-line* maupun *off-line*.

Seperti yang telah di bahas pada bagian 2 butir H bahwa Bank X selaku penerbit kartu kredit sejak tahun 1997, telah melakukan *self-regulatory* dalam meminimalisir dan mengelola risiko-risiko fraud carding dan penanganannya secara komprehensif. Prosedur penanganan fraud akibat carding dalam Bank X adalah sebagai berikut[2]:

1. Bank X menerima pengaduan dari nasabah atau pemegang kartu bahwa yang bersangkutan melaporkan **transaksi e-commerce yang janggal** yang tertera pada lembar tagihan (billing statement) bulan berjalan.
2. Petugas customer service Bank X segera menindaklanjuti dengan melaporkannya pada kesempatan pertama kepada bagian RMU (Risk Management Unit).
3. Staf RMU membaca laporan terlebih dahulu lalu mengolahnya dan kemudian melakukan blokir kartu dengan kode “F” pada sistem mainframe yang bernama Card Link.
4. Kemudian petugas RMU segera menindaklanjuti laporan nasabah dengan melakukan investigasi internal dan eksternal.

[2] Hasil Wawancara dengan Sdr. Wilhelmus Max dari Bagian RMU tanggal 08 Oktober 2010, jam 17.30 wib

12. MEKANISME *CHARGEBACK* DI BANK X

Chargeback adalah suatu mekanisme beban balik akibat transaksi fraud yang tidak dilakukan oleh pemegang kartu kredit yang sah. Mekanisme beban balik telah menjadi mekanisme lazim dalam industri kartu kredit, dimana terdapat dua pihak pelaku beban balik yakni:

a. Pihak bank sebagai *issuer*
b. Pihak bank sebagai *acquirer*

Pihak issuer akan melakukan pembebanan atas sejumlah nominal transaksi kepada pihak acquirer karena toko mereka telah memfasilitasi dan atau membuka peluang bagi terjadinya transaksi fraud. Dengan beban balik ini pihak issuer akan mendapatkan dananya kembali yang kemudian dapat digunakan untuk menghapus transaksi dari pemegang kartu kredit bank tersebut. Eksekusi chargeback dijalankan secara elektronik dengan menggunakan sarana komunikasi elektronik Card Link yang terkoneksi ke jaringan Visa dan atau MasterCard.

Mekanisme *chargeback* diatur oleh Visa atau Mastercard dengan contoh regulasi dari pihak *principal* sebagai berikut:

> *Regulasi No. 3.24.1.2 Periode Waktu bagi Issuer untuk melakukan Chargeback*
> *Issuer dapat melakukan beban balik secara layak atas transaksi fraud yang terjadi pada pemegang kartu yang tertera dalam Global Security Bulletin selama periode beban balik itu masih berlaku dalam Global Security Bulletin. Beban balik harus disampaikan tidak lebih dari 120 hari kalender setelah tanggal publikasi pertama Global Security Bulletin yang mencantumkan lokasi merchant atau dalam rentang waktu 120 hari kalender dari tanggal transaksi Central Site Business.*

Adapun pengajuan teknis chargeback tersebut juga diatur oleh Visa atau MasterCard dengan regulasi sebagai berikut:

> *Regulasi No. 3.33.1 Pemakaian Kode Pesan Yang Cocok 4863*
> *Issuer dapat menggunakan kode alasan atau pesan nomor 4863 untuk seluruh transaksi carding (pihak Prinsipal menyebut Carding sebagai Card Not Present Transaction) apabila:*
> - *Pemegang kartu mengklaim bahwa dia tidak mengenali adanya transaksi yang muncul dalam lembar tagihan ybs.*
> - *Issuer telah melakukan usaha-usaha yang cukup baik untuk mengidentifikasikan transaksi itu bagi pemegang kartu. (Contoh: Issuer mengkonfirmasi bahwa pemegang kartu berusaha atau telah menghubungi merchant untuk mendapatkan identifikasi transaksi).*
> - *Issuer harus menginstruksikan pemegang kartunya untuk menghubungi merchant untuk mendapatkan informasi lebih lanjut sebelum mereka melakukan chargeback.*

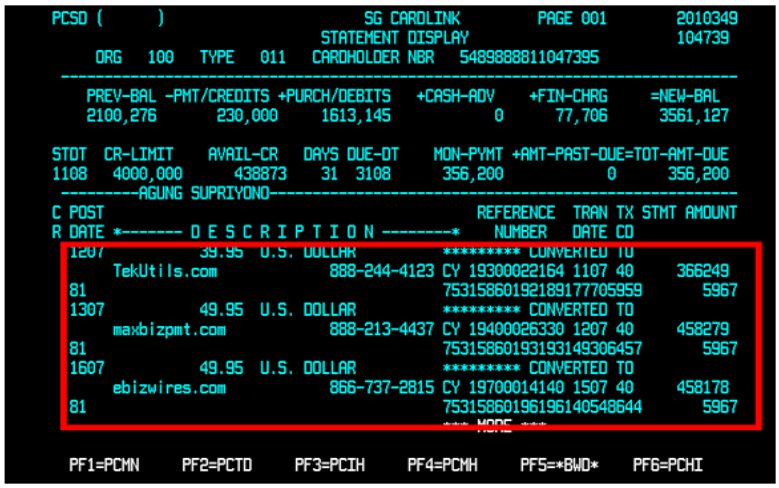
13. CONTOH PENANGANAN KASUS CARDING BANK X ATAS NAMA AGUNG S

Pada tanggal 30 Agustus 2010, seorang nasabah Bank X bernama Agung S melaporkan pengaduan (*complaint*) bahwa ybs menyangkal (*dispute*) transaksi belanja Internet yang tertera dalam lembar tagihan bulan Agustus 2010. Terdapat 4 (empat) transaksi yang mencurigakan dengan total Rp. 1.738.860,-, dengan rincian sebagai berikut:

1. Transaksi di www.tekutils.com tanggal 11 Juli 2010 dengan nilai transaksi Rp. 366.249,-
2. Transaksi di www.maxbizpmt.com tanggal 12 Juli 2010 dengan nilai transaksi Rp.458.279,-
3. Transaksi di www.ebizwires.com tanggal 15 Juli 2010 dengan nilai transaksi Rp.458.178,-

Transaksi di www.maxbizpmt.com tanggal 12 Agustus 2010 dengan nilai transaksi Rp.456.154,-

Dalam screen Card Link Bank X dengan jelas tertera transaksi yang mencurigakan tersebut, sebagai berikut:

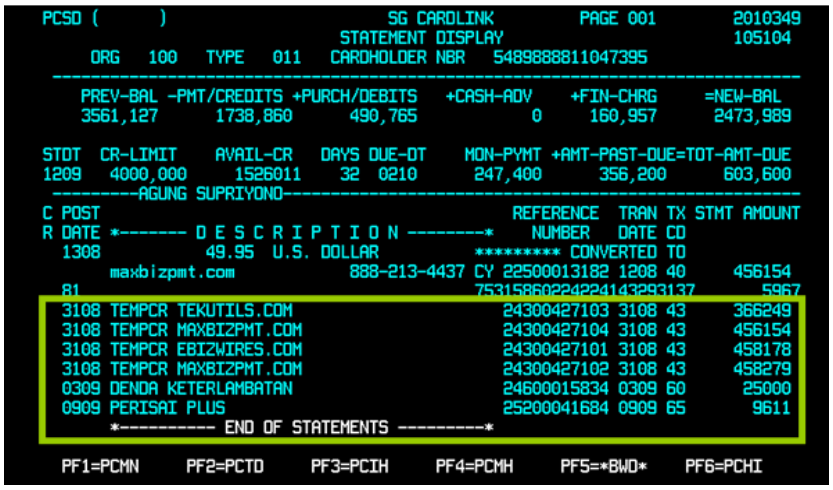


Gambar 4 Transaksi Carding Nasabah (kotak garis merah)

Petugas RMU Bank X segera melakukan investigasi berdasarkan prosedur yang telah ditetapkan. Dari investigasi diperoleh kesimpulan bahwa nasabah a.n Agung S adalah korban carding. Hal ini diketahui bahwa selama menjadi pemegang kartu kredit ybs tidak pernah melakukan transaksi belanja di Internet. Tren transaksi yang dicek-silang adalah transaksi-transaksi sebelum terjadinya fraud Carding. Beberapa sampel transaksi ybs dianalisa oleh petugas RMU Bank X.

Setelah menyimpulkan bahwa Agung S menjadi korban kejahatan Carding maka Bank X segera melakukan tindak lanjut dengan melakukan *chargeback* ke merchant di luar negeri. Empat transaksi carding berlangsung di merchant yang berada di Eropa. Dari penelusuran menggunakan teknik *who is domain* di http://whois.domaintools.com diperoleh bahwa merchant berada di Cyprus dengan alamat di *Registrant Nomor: [2797768]; Web Admin : legal@taraliatradingltd.com, Taralia Trading Ltd , Agias Fylaxeos & Zinonos Rossidi, 21st floor, Limassol Cyprus, 3082 CY.*

Dari kejadian Carding di atas, Bank X akhirnya melakukan tindakan *chargeback* dan selanjutnya melakukan peng*credit*-an secara akuntasi sehingga tagihan transaksi tersebut dihapuskan dari tagihan ybs. Hal ini terlihat dari screen Card Link berikut :



Gambar 5 Penghapusan Transaksi Carding (kotak garis hijau)

Proses penghapusan 4 (empat) transaksi carding dengan total nominal sebesar Rp 1.738.860. telah dilakukan pada tanggal 31 Agustus 2010 pada periode lembar tagihan September 2010. Artinya tindaklanjut penyelesaian transaksi carding untuk melindungi kepentingan nasabah hanya memakan waktu 1 (satu) hari sejak pemegang kartu a.n Agung S mengadukan masalah ini tanggal 30 Agustus 2010.

Sementara itu, untuk kartu kredit pengganti (*replacement card*) dilakukan pada tanggal 13 Desember 2010. Proses penggantian yang lama ini untuk menyelesaikan secara tuntas dan legal terutama untuk memenuhi kelengkapan fisik dokumen (sales draft). Hal ini tidak mudah mengingat terdapat 4 transaksi dengan 3 merchant yang berada di luar negeri. Sehingga sesuai regulasi MasterCard No. 3.24.1.2 diperbolehkan memproses tuntas paling lambat 120 hari kalender sejak nasabah pertama kali *complaint.*

Jadi dengan melakukan penggantian kartu kredit baru, nabasah a.n Agung S berdasarkan regulasi MasterCard dan kebijakan Bank X telah mendapatkan perlindungan yang memadai dari pihak perbankan. Kasus Carding tersebut telah dinyatakan ”cased closed”. Kerugian nasabah dalam kasus Agung S menjadi kerugian Bank X. Bank X juga telah melakukan *chargeback* kepada *acquiring bank* di Cyprus tersebut. Secara umum kasus carding pada transaksi internet Bank X selama Januari 2009 – Desember 2010 sebagai berikut:

Tabel 3 Besar Situs Transaksi Carding Bank X – Akumulatif Jan 2009 – Des 2010

No	TRX	Amount (Akumulatif)
1	WWW.MANDALAAIR.COM	Rp 124.058.032
2	Amazon.com	Rp 75.341.312
3	www.freelife.com	Rp 73.807.850
4	WWW.ENTROPAY.COM	Rp 64.379.076

5	OCTOPUSTRAVEL.COM	Rp 43.792.733
6	MCAFEE.COM	Rp 38.832.234
7	WWW.SKYPE.COM	Rp 31.387.130
8	MB*MONEYBOOKERS.COM	Rp 27.895.554
9	AGODA.COM	Rp 27.338.358
10	WWW.ASIATRAVEL.COM	Rp 25.679.369
11	QATAR AIRWAYS (E.COMMERCE	Rp 23.568.748
12	ABEBOOKS.COM	Rp 23.488.076
13	FACEBOOK.COM*CREDITS	Rp 22.578.359
14	CALPOP.COMINC	Rp 22.219.209
15	MY-INTERNET-PAYDAY.COM	Rp 20.094.898
16	WWW.AIRARABIA.COM	Rp 19.571.169
17	LASTMINUTE.COM	Rp 19.374.918
18	WOTIF.COM HOTELS	Rp 18.860.754
19	GTA-TRAVEL.COM	Rp 18.843.085
20	GODADDY.COM	Rp 18.803.744
GRAND Total		**Rp 739.914.608**

14. UPAYA-UPAYA PENCEGAHAN KASUS CARDING BANK X

Dari kebijakan bank X di atas maka bank tersebut melakukan berbagai upaya pencegahan carding sehingga dampak fraud dapat diminimalisir. Memang *zero fraud* akan sangat sulit tercapai, meskipun bukan mustahil, mengingat kasus-kasus carding terjadi juga karena kelalaian kastemer sehingga data kartu kreditnya baik secara sengaja maupun tidak sengaja bocor ke beberapa pihak.
Oleh karena itu Bank X membuat upaya-upaya pencegahan dengan cara sebagai berikut:

1. Membentuk tim *Early Detection Unit* (EDU) pada pertengahan tahun 2007. Tim ini terdiri dari beberapa personel Bank X yang bertugas untuk memantau, menganalisa dan mengambil tindakan yang diperlukan untuk mengurangi risiko carding. Tim EDU dalam aktivitasnya selalu menghubungi kastemer untuk memastikan apakah transaksi on-line itu benar adanya dilakukan oleh yang bersangkutan.
2. Melakukan sosialisasi pencegahan fraud termasuk risiko carding. Sosialisasi dilakukan ke seluruh pemegang kartu Bank X dengan membuat pesan-pesan edukasi di lembar tagihan, pengiriman SMS, dan pengiriman surat khusus ke kastemer yang bersifat tematik.
3. Memperkuat keamanan (*security*) sistem card link dan mesin-mesin EDC yang dimiliki oleh Bank X dengan cara membuat enskripsi dan masking pada struk/slip transaksi di merchant-merchant. Proses masking (tanda bintang: *******) dimaksudkan untuk menutupi atau mengaburkan informasi nomor kartu kredit yang muncul pada lembar struk sehingga tidak berpotensi dipergunakan oleh carder dalam aksi-aksi carding mereka. Contoh masing sebagai berikut:


UMB KAMPUS MENTENG
GEDUNG TEJA BUANA
JL.MENTENG RAYA NO.29 JAKARTA 10340

TERMINAL ID. : 29597201
MERCHANT #: 000100012095922

MASTER
**********3344 (Insert)
LEONARD T P
AID: A0000000041010
EMV SALE EXP. : 07/12
BATCH: 000160 TRACE: 362936
DATE : 13/11/10 TIME : 10:05
REF# : 000011002535 APPRV: R98558

TOTAL RP.1.824.500

X
I AGREE TO PAY ABOVE TOTAL AMOUNT
ACCORDING TO CARD ISSUER AGREEMENT
MERCHANT AGREEMENT IF CREDIT VOUCHER

Gambar 6 Struk Bank X yang sudah di*masked*

Dari upaya-upaya pencegahan carding di atas maka terjadi penurunan jumlah kasus carding termasuk penurunan nilai transaksi carding secara signifikan. Data transaksi carding Bank X sebagai berikut:

Tabel 4 Penurunan Jumlah Transaksi Carding

Tahun	# Transaksi Carding	% Turun
2008	2.431	0,00%
2009	2.124	**-12,63%**
2010	1.332	**-37,29%**

Penurunan jumlah transaksi diakibatkan karena pencegahan risiko carding yang dijalankan secara optimal oleh Bank X terutama tim EDU. Jadi hipotesa bahwa Bank X telah melakukan upaya pencegahan dan penanganan carding secara sungguh-sungguh dapat diterima.

15. PERLINDUNGAN NASABAH KASUS CARDING DALAM UU ITE NO.11 TAHUN 2008

Perlindungan hukum bagi nasabah pengguna kartu kredit mutlak diperlukan seperti halnya perlindungan yang diberikan kepada nasabah penyimpan dana lainnya. Menurut sistem perbankan Indonesia, perlindungan terhadap nasabah dapat dilakukan melalui dua metode, yaitu:

a. Perlindungan secara eksplisit (*explicit deposit protection*)
   Yaitu perlindungan yang diperoleh melalui pembentukan lembaga yang menjamin simpanan masyarakat, sebagaimana diatur dalam Keputusan Presiden No. 26 Tahun 1998 tentang Jaminan terhadap Kewajiban Bank Umum. Sehingga apabila bank mengalami kegagalan, maka lembaga tersebut akan mengganti dana masyarakat yang disimpan dalam bank yang

gagal tersebut. Hal ini diatur dalam Keputusan Presiden No. 26 Tahun 1998 tentang Jaminan terhadap Kewajiban Bank Umum, sebelum diberlakukannya asuransi deposito (Marulak Pardede, 2001).

b. Perlindungan secara implisit (*implicit deposit protection*)
Yaitu perlindungan yang dihasilkan oleh pengawasan dan pembinaan bank secara efektif. Maksudnya agar dapat menghindari terjadinya kebangkrutan bank yang diawasi. Perlindungan semacam ini dapat diperoleh melalui (Marulak Pardede, 2001):
   1) Peraturan perundang-undangan di bidang ITE dan perbankan;
   2) Perlindungan yang dihasilkan oleh pengawasan dan pembinaan yang efektif, yang dilakukan oleh Bank Indonesia;
   3) Upaya menjaga kelangsungan usaha bank sebagai suatu lembaga pada khususnya dan perlindungan terhadap sistem perbankan pada umumnya;

Sementara itu dalam UU ITE No.11 tahun 2008 memang tidak menyebutkan secara eksplisit tindak pidana carding namun Undang-undang ini dalam penjelasannya menyatakan secara eksplisit bahwa kegiatan siber (cyber) tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapan pun dan dari mana pun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya **pencurian dana kartu kredit** melalui pembelanjaan di Internet.

Oleh karena itu UU ITE No.11 tahun 2008 secara jelas mengatur perlindungan warga negara dari tindak pidana kejahatan yang berhubungan dengan transaksi elektronik baik melalui penegakan hukum perdatan maupun hukum pidana. Untuk kasus carding yang merupakan transaksi elektronik yang dilakukan secara *non face to face* maka perlindungan nasabahnya diatur oleh Pasal 32 dengan sanksi pidananya berada pada Pasal 48. Kasus carding berhubungan dengan pencurian data dan informasi kartu kredit. Meskipun tidak ada kata "pencurian" dalam UU ITE No.11 tahun 2008 namun pengaturan carding mengacu secara spesifik pada Pasal 32 ayat 1 sebagai berikut:

> *Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik Publik.*

Dalam kasus-kasus carding dimana nomor kartu kredit tersebar luas dan dapat diakses oleh publik maka pengaturan dalam UU ITE No.11 berada pada Pasal 34 ayat 1 butir b dengan bunyi sebagai berikut:

> *Sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.*

Masalah yang akan banyak memusingkan pengguna Internet adalah Bab VII mengenai Perbuatan yang dilarang yang terdapat dalam Pasal 27-37 UU ITE, semua pasal ini menggunakan kalimat setiap orang. Padahal perbuatan yang dilarang, seperti *spam*, penipuan, *cracking*, virus, penipuan, *spam*, *flooding* sebagian besar akan dilakukan oleh mesin dengan algoritma program jahat.

Bahkan sering kali penjalaran *spam, worm* bukan dilakukan oleh programer pada tangan pertama.

Secara sepintas UU ITE dapat memperkecil ruang gerak *hacker* yang melakukan pengrusakan dan melakukan pencurian nomor kartu kredit melalui Internet atau carding. Memang cakupan atau ruang lingkup UU ITE sangat luas sebagai *lex generalis* (payung hukum) bagi tindak pidana di bidang elektronika, teknologi informasi dan komunikasi. Namun demikian luasnya cakupan tersebut harus juga dibarengi dengan pengaturan yang spesifik di bidang tindak pidana carding ini. Mengingat RUU TIPITI sudah berada di lembaga legislasi DPR untuk nantinya dirumuskan menjadi UU maka pihak legislator perlu mendapatkan masukan yang memadai dari pelaku industri kartu kredit di Tanah Air.

Oleh karena itu dari berbagai kasus yang muncul di kalangan bank-bank issuer dalam negeri dan khususnya pembahasan penanganan praktek carding di Bank X maka UU ITE No.11 tahun 2008 perlu menambahkan secara eksplisit beberapa pengaturan atau formulasi hukum sebagai berikut:

1) Tindak pidana memperjual-belikan data dan membocorkan informasi kartu kredit. Hal ini untuk mengantisipasi pertukaran data yang terjadi dalam praktek perbankan dan lembaga keuangan lainnya. Presedensi ini dapat ditemukan dari bocornya data kartu kredit ketika nasabah boleh mengajukan aplikasi kartu kredit ke beberapa bank. Singkatnya nasabah yang sudah eksis di bank X boleh mengajukan aplikasi kartu kredit di Bank Y. Orang-orang yang tak berhak membaca informasi dari aplikasi bank Y tersebut akan dengan mudah melakukan carding. Hal ini terjadi karena untuk mendapatkan kartu kredit di Bank Y, cukup melampirkan copy kartu kredit bank X atau mengisi kolom kepemilikan kartu kredit di bank sebelumnya.
2) Tindak pidana bagi para pelaku dalam jaringan transaksi kartu kredit. Hal ini dapat terjadi mengingat bocornya informasi kartu kredit dapat terjadi di berbagai titik *network* seperti perusahaan jasa cetak kartu kredit, pihak kurir, merchant (kasir dan pegawai lainnya), perusahaan switching serta provider jaringan komunikasi data.
3) Tindak pidana bagi setiap orang atau organisasi atau mesin yang menyediakan fasilitas atau sarana untuk melakukan pembocoran dan penyadapan data kartu kredit. Hal ini untuk mengantisipasi setiap usaha yang dijalankan termasuk keberadaan warnet sebagai sarana tempat berkumpulnya para carder dalam melakukan aksi-aksinya. Hal ini juga termasuk kegiatan men*download* dan meng*upload* sofware-software generator kartu kredit.

16. KESIMPULAN

Berdasarkan uraian serta analisis hasil penelitian yang telah dijabarkan pada bagian terdahulu maka pada bagian ini dapat ditarik kesimpulan sebagai berikut :

1. Perkembangan teknologi on line di dunia maya termasuk regulasi kartu kredit telah diatur sejumlah instrumen hukum dan peraturan sebagai berikut:

a. Peraturan Bank Indonesia, PBI Nomor: 7/52/PBI/2005 dan PBI Nomor: 11/11/PBI/2009 Tentang Penyelenggaran Kegiatan Alat Pembayaran Menggunakan Kartu.
b. Peraturan Bank Indonesia, PBI No. 9/15/PBI/2007 tentang Penerapan Manajemen risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum.
c. UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. *Cyber crime* memiliki beberapa bentuk dalam aktivitasnya dalam bidang perbankan. Khusus industri kartu kredit, bentuk kejahatan di internet yang melibatkan transaksi fraud adalah *carding*. Oleh karena itu UU ITE No.11 tahun 2008 merupakan payung hukum yang relevan bagi penanggulangan kejahatan dunia maya pada umumnya dan kejahatan carding pada khususnya.
3. Perlindungan nasabah sangat penting guna menciptakan kondisi yang saling menguntungkan antara berbagai pihak dalam meningkatkan nilai transaksi e-commerce di Indonesia. Perlindungan nasabah dalam mengantisipasi dan menangani kasus-kasus carding antara lain: Pasal 32 dan 48 UU ITE No.11 tahun 2008.

Bank X telah melakukan upaya-upaya internal melalui kebijakan bank (antara lain mekanisme *chargeback* dan pembentukan tim *Early Detection* Unit atau disingkat dengan *tim EDU*) untuk melindungi kepentingan nasabah dalam menghindari dan menuntaskan kejahatan carding.

17. SARAN

1. Perlu segera diupayakan sosialisasi *cyber law* di Indonesia yang dapat menunjang pemakaian kartu kredit sebagai alat pembayaran dalam transaksi on line secara bertanggung jawab dan memiliki dasar hukum yang kuat.
2. Terdapat wacana RUU TIPITI (Tindak Pidana Teknologi dan Informasi) yang saat ini keberadaannya di lembaga legislasi DPR. RUU TIPITI dalam Pasal 13 mengatur masalah penyalahgunaan transaksi elektronik menggunakan kartu kredit. Oleh karena itu, RUU TIPITI juga dapat dipandang sebagai *lex specialis* bagi penegakan hukum dalam kejahatan carding. Di masa mendatang aturan RUU TIPITI harus dioptimalkan dengan menambahkan pasal-pasal seperti jual-beli data kartu kredit, pemakaian software dan program-progam komputer yang jahat untuk mendapatkan nomor dan data kartu kredit secara melawan hukum.

DAFTAR PUSTAKA

1. Buku

Amiruddin dan Zainal Asikin, *Pengantar Metode Penelitian Hukum*, Jakarta: Grafitti Press, 2006.

Hamzah, Andi, *Aspek-Aspek Pidana di Bidang Komputer*, Jakarta: Sinar Grafika, 1989.

Ibrahim, Johnny *Teori dan Metodologi Penelitian Hukum Normatif*, Bandung: Citra Aditya Bakti, 2007.

Koentjaraningrat, *Metode-Metode Penelitian Masyarakat*, Jakarta: Prenada Media, 1997.

Magdalena, Merry dan Maswigrantoro Roes Setiyadi, *Cyberlaw, Tidak Perlu Takut?*, Yogyakarta: ANDI, 2007.

Marzuki, Peter Mahmud, *Penelitian Hukum*, Jakarta: Kencana Media Group, 2005.

Muhammad, Abdulkadir dan Rilda Murniati, *Segi Hukum Lembaga Keuangan dan Pembiayaan*, Jakarta: Citra Aditya Bakti, 2000.

Rahardjo, Agus, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: PT. Citra Aditya Bakti, 2002.

Supranto, J, *Metode Penelitian Hukum dan Statistik*, Jakarta: Pradnya Paramitha, 2003.

Wisnubroto, Aloysius, *Strategi Penanggulangan Kejahatan Telematika*, Yogyakarta: Penerbit Atmajaya Yogyakarta, 2010.

Wong, K. Daniel, *Wireless Internet Telecommunication*, Artech House Mobile Communication, 2005.

2. Peraturan Perundang-undangan dan Regulasi

Bank X, *Pedoman Perusahaan dan Kebijakan Kartu Kredit*, Jakarta: 2010

International Télécommunications Union, *ITU ToolKit for Cybercrime Legislation - Section 5. Interception*, Draft Rev. February 2010.

Mastercard International, *Security Rules and Procedures*, MO-USA, 2003.

Mastercard International, *Chargeback Guide and Policy*, MO-USA, 2003.

Republik Indonesia, Kitab Undang-undang Hukum Pidana

Republik Indonesia, Peraturan Bank Indonesia No.11/11/PBI/2009 tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu.

Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, dan Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Republik Indonesia, Undang-Undang No. 10 Tahun 1998 mengenai Perubahan Undang-undang Nomor 7 Tahun 1992 tentang *Perbankan*, LN No.182 Tahun 1999.

Republik Indonesia, Draft Rancangan Undang-Undang Tindak Pidana Teknologi Informasi, diunduh dari http://www.free.vlsm.org/v17/com/ictwatch/data/ruu-tipiti-final.doc, tanggal akses 02 April 2010.

3. Laporan/Jurnal/Artikel

Bank Indonesia, *Laporan Sistem Pembayaran dan Pengedaran Uang*, Jakarta: BI, 2009.

Bank X, *Business Presentation Report*, Jakarta: Card Center Bank X, 2009.

Bank X, *Bahan Pelatihan Bank X Card Center - EDC dan Network*, 2009.

IEEE Symposium on Security and Privacy, Journal: *Chip and PIN is Broken*, Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond, University of Cambridge, UK, 2010.

Pardede, Marulak "Efektivitas Pengawasan Perbankan dalam Perbankan Nasional", Jakarta: Majalah Jurnal Hukum Bisnis, edisi September 2001.

Verisign, *Internet Security Intelligence Briefing*, Dulles VA USA, 2004.

4. Internet

Adiputra, Yoga, "Artikel Ekonomi", Dikutip dari http://www.kompas.com, Diakses tanggal 3 April 2009.

C12-08, Penulis, "Kompas Tekno", Dikutip dari http://www.kompas.com, Diakses tanggal 01 Oktober 2010.

Prayogi, Whery Enggo, Dikutip dari

http://www.detikfinance.com/read/2010/11/09/134811/1490195/5/perbankan-kesulitan-bendung-praktik-jual-beli-data-nasabah-kartu-kredit, tanggal akses 19 November 2010, jam 10.30 wib

Purnomo, Herdaru, Dikutip dari http://www.detikfinance.com/read/2010/10/20/081525/1469578/5/bikin-npl-naik-bi-khawatirkan-maraknya-gestun-kartu-kredit?f9911013, tanggal akses 20 Oktober 2010, jam 14.00 wib

Sutadi, Heru, "UU ITE dan Tantangan Cybercrime", Dikutip dari http://nasional.kompas.com/read/2008/04/17/02300074/UU.ITE.dan.Tantangan..quot.Cybercrime.quot., Diakses tanggal 10 Juni 2008.

Syurkani, Panca, "Artikel Metro", Dikutip dari http://www.tempointeraktif.com, Diakses tanggal 01 Agustus 2010.