

Ringkasan Eksekutif
Diskusi Permasalahan Hukum Terkait *Internet Banking*
dan Solusi Penyelesaiannya*
(Brian Ami Prastyo, S.H., MLI)

Internet Banking kini bukan lagi istilah yang asing bagi masyarakat Indonesia khususnya yang tinggal di wilayah perkotaan. Hal tersebut disebabkan semakin banyaknya perbankan nasional yang menyelenggarakan layanan tersebut. Di masa mendatang, layanan ini tampaknya sudah bukan lagi sebuah layanan yang akan memberikan *competitive advantage* bagi bank yang menyelenggarakannya. Keadaannya akan sama seperti pemberian fasilitas ATM. Semua bank akan menyediakan fasilitas tersebut. Namun demikian, tampaknya di balik perkembangan ini terdapat berbagai permasalahan hukum yang mungkin di kemudian hari dapat merugikan masyarakat jika tidak diantisipasi dengan baik. Diskusi ini mencoba mengidentifikasi berbagai permasalahan tersebut dan alternatif pemecahannya.

A. Identifikasi Permasalahan

1. Keamanan Sistem Informasi

Bisnis perbankan pada dasarnya merupakan bisnis yang berisiko tinggi. Terdapat sedikitnya 8 macam risiko utama yang berkaitan dengan aktivitas perbankan, yaitu strategi, reputasi, operasional (termasuk yang disebut risiko transaksi dan legal), kredit, harga, kurs, tingkat bunga, dan likuiditas. Penyelenggaraan *Internet Banking* yang sangat dipengaruhi oleh perkembangan teknologi informasi, dalam kenyataannya pada satu sisi membuat jalannya transaksi perbankan semakin mudah, akan tetapi di sisi yang lain membuatnya juga semakin berisiko. Dengan kenyataan seperti ini, faktor keamanan harus menjadi faktor yang paling perlu diperhatikan. Bahkan mungkin faktor keamanan ini dapat menjadi salah satu fitur unggulan yang dapat ditonjolkan oleh pihak bank.

* Diskusi ini terselenggara di Jakarta, 22 Maret 2005, atas kerjasama Bank Indonesia dengan LKHT FHUI

Aktivitas *Internet Banking* meningkatkan dan memodifikasi risiko-risiko seperti strategi, operasional dan reputasi. Hal ini disebabkan risiko tersebut terkait langsung dengan ancaman terhadap aliran data yang *reliable* dan semakin kompleksnya teknologi yang menjadi dasar *Internet Banking*. Ancaman tersebut dapat dikelompokkan sedikitnya menjadi *Accidental Ancamans*, *Intentional Ancamans*, *Passive Ancamans*, dan *Active Ancamans*. Seiring dengan meningkatnya pemanfaatan *Internet Banking*, akan semakin banyak pihak-pihak yang mencari kelemahan sistem *Internet Banking* yang ada. Serangan-serangan tersebut akan semakin beragam jenisnya dan tingkat kecanggihannya. Bila dahulu serangan tersebut umumnya bersifat pasif, misalnya *eavesdropping* dan *offline password guessing*, kini serangan tersebut menjadi bersifat aktif, dalam arti penyerang tidak lagi sekedar menunggu hingga *user* beraksi, akan tetapi mereka beraksi sendiri tanpa perlu menunggu *user*. Beberapa jenis serangan yang dapat dikategorikan ke dalam serangan aktif adalah *man in the middle attack* dan *trojan horses*.

Berbagai upaya preventif memang telah diterapkan oleh kalangan perbankan di Indonesia yang menyelenggarakan layanan *Internet*

Banking. Misalnya, dengan diberlakukannya fitur *two factor authentication*, dengan menggunakan token. Penggunaan token ini akan memberikan keamanan yang lebih tinggi dibandingkan bila hanya menggunakan *username*, *PIN*, dan *password* saja. Akan tetapi dengan adanya penggunaan token ini, tidak berarti transaksi *Internet Banking* bebas dari risiko. Serangan yang bersifat aktif seperti *man in the middle attack* dan *trojan horses* dapat mengganggu keamanan layanan. Gambaran umum dari aktifitas yang sering disebut *man in the middle attack* adalah sebagai berikut: penyerang membuat sebuah *website* dan membuat *user* masuk ke *website* tersebut. Agar berhasil mengelabui *user*, *website* tersebut harus dibuat semirip mungkin dengan *website* bank yang sebenarnya. Kemudian *user* memasukkan *passwordnya*, dan penyerang kemudian menggunakan informasi ini untuk mengakses *website* bank yang sebenarnya. Untuk mengecoh token, penyerang dapat mengirimkan *challenge-response* kepada *user* sebelum melakukan transaksi illegal. Sedangkan, *trojan horses* adalah program palsu dengan tujuan jahat, yang disusupkan kepada sebuah program yang umum dipakai. Di sini para penyerang meng-install *trojan* kepada komputer *user*. Ketika *user login* ke *website* banknya, penyerang

menumpang sesi tersebut melalui *trojan* untuk melakukan transaksi yang diinginkannya.

Beberapa bentuk serangan yang dapat mengganggu penyelenggaraan *Internet Banking* adalah sebagai berikut:

- *Masquerade*
- *Reply*
- *Cable sniffing*
- *Traffic analysis*
- *Outsider attack*
- *Insider attack*
- *Viruses*
- *Dictionary attack*
- *Modification of messages*
- *Trapdoor*
- *Theft*
- *Electronic eavesdroppin*
- *Denial of Service*
- *Trojan horse*
- *Exhaustion attack*
- *Natural ancamans*

Dengan mencermati data penyalahgunaan jaringan informasi (*network abuse*) yang dikeluarkan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) sepanjang Januari 2003 sampai dengan Agustus 2004, tampak bahwa berbagai ancaman terhadap keamanan sebagaimana dikemukakan di atas adalah riil. Bahkan ancaman tersebut sebenarnya dapat lebih besar lagi, mengingat 'fenomena gunung es' juga terjadi dalam hal ini. Hal ini karena data yang ada dalam laporan tampaknya berbeda dengan fakta di lapangan yang dirasakan masyarakat.

Bulan	Network Incident	Abuse Open Proxy	Fraud
Jan-03	89	n/a	5
Feb-03	76	n/a	5

Mar-03	100	n/a	7
Apr-03	511	n/a	6
Mei-03	523	n/a	4
Jun-03	344	n/a	7
Juli-03	188	n/a	5
Agst-03	153	n/a	6
Sept-03	114	n/a	4
Oct-03	88	502	9
Nov-03	43	457	67
Des-03	38	251	85
Jan-04	92	358	18
Feb-04	69	492	0
Mar-04	122	685	3
Apr-04	75	485	8
Mei-04	89	234	1
Jun-04	95	371	8
Juli-04	89	21	5
Agst-04	147	383	3

Namun demikian, penting juga untuk diingat bahwa seringkali kerusakan atau kegagalan dari sistem komputer dan data tidak diakibatkan oleh serangan yang datang dari luar, tetapi terjadi karena hal yang sangat sederhana. Misalnya, tindakan yang tidak benar atau menyimpang yang dilakukan oleh pemakai yang sah (nasabah atau pegawai) dari sebuah sistem. Dengan kata lain, kerugian atau kehilangan yang diderita oleh bank atau nasabah dapat juga diakibatkan oleh petugas internal atau manajemen bank, misalnya dengan mengambil dan menggunakan identitas nasabah serta melakukan rekayasa laporan keuangan bank.

2. Kejahatan Lama Dengan Cara Baru

Ada dua kegiatan perbankan di Internet yang potensial menjadi target *cybercrime*. Kegiatan yang pertama, yaitu layanan pembayaran menggunakan kartu kredit pada toko-toko *online*. Sistem layanan ini rentan terhadap tindak kejahatan yang dikenal dengan istilah *carding*. Sampai saat ini, sedikitnya terdapat 4 modus *carding* yang telah dikenali, yaitu **Modus I (1996 – 1998)**, para *carder* mengirimkan barang hasil *carding* mereka langsung ke suatu alamat di Indonesia. **Modus II (1998 – 2000)**, para *carder* tidak lagi secara langsung menuliskan “Indonesia” pada alamat pengiriman, tetapi menuliskan nama negara lain. Kantor pos negara lain tersebut akan meneruskan kiriman yang “salah tujuan” tersebut ke Indonesia. Hal ini dilakukan oleh para *carder* karena semakin banyak *merchant* atau perusahaan penyedia *e-commerce* di Internet yang menolak mengirim produknya ke Indonesia. **Modus III (2000 – 2002)**, para *carder* mengirimkan paket pesanan mereka ke rekan mereka yang berada di luar negeri. Kemudian rekan mereka tersebut akan mengirimkan kembali paket pesanan tersebut ke Indonesia secara normal dan legal. Hal ini dilakukan oleh *carder* selain karena modus operandi mereka mulai

tercium oleh aparat oleh aparat penegak hukum, juga disebabkan semakin sulit mencari *merchant* yang biasa mengirim produknya ke Indonesia. **Modus IV (2002 – sekarang)**, para *carder* lebih megutamakan untuk mendapatkan uang tunai. Caranya adalah dengan mentransfer sejumlah dana dari kartu kredit bajakan ke sebuah rekening di www.PayPal.com. Kemudian dari PayPal, dana yang telah terkumpul tersebut dikirimkan oleh pelaku ke rekening bank yang diinginkan. Cara lainnya adalah dengan melakukan penipuan, seolah-olah *carder* menjual barang hasil *carding*, dan menjebak korban dengan meminta mengirimkan uang muka dalam jumlah tertentu. Namun, masih terdapat pula para *carder* yang tetap melakukan modus I, II, dan III, terutama bagi pemula.

Secara non-materiil akibat yang ditimbulkan dari tindakan penyalahgunaan kartu kredit adalah sebagai berikut:

- a. Penilaian dunia terhadap Indonesia menjadi negatif, karena dari hasil riset tahun 2001 dan 2003, Indonesia menempati peringkat ke-2 dunia dalam *credit card fraud world cyber* (<http://www.clearcommerce.com>).
- b. Dengan peringkat ke-2 tersebut, banyak transaksi dari Indonesia (termasuk yang legal) ditolak oleh perusahaan-perusahaan

(*merchant*), sehingga secara tidak langsung akan memengaruhi perekonomian negara serta *image* bangsa di pergaulan antar bangsa.

- c. Kepercayaan masyarakat dan dunia usaha akan turun serta berusaha mencari cara lain dalam bertransaksi atau mencari bank penerbit kartu kredit lain yang terjamin keamanannya.
- d. Langsung maupun tidak langsung konsumen atau pelanggan kartu kredit akan was-was setiap akan bertransaksi serta buang-buang waktu karena setiap saat selalu mengecek dana yang masih tersimpan di kartu kreditnya.

Sedangkan secara materiil, kerugian yang mungkin timbul adalah:

- a. Terambilnya dana yang jumlahnya sangat bervariasi serta tidak dapat diduga/terpikirkan sebelumnya, baik oleh pemilik kartu kredit maupun oleh *issuing bank*.
- b. Bila hal itu menimpa banyak pemilik kartu kredit dapat dibayangkan betapa besar nilai uang yang diambil para *carder* tersebut.
- c. *Issuing bank* harus sering mengeluarkan kartu kredit baru sebagai pengganti kartu kredit milik korban *credit card fraud*.

Kegiatan yang kedua yaitu perbankan *online* (*online banking*), juga relatif rentan terhadap *cybercrime*. Modus yang pernah muncul di Indonesia dikenal dengan istilah *typosite*. Modus ini memanfaatkan nasabah yang salah mengetikkan alamat bank *online* yang ingin diaksesnya. Pelakunya sudah menyiapkan situs palsu yang mirip dengan situs asli bank *online* (*forgery*). Jika ada nasabah yang salah ketik dan kesasar di situs bank palsu tersebut, pelaku akan merekam *user id* dan *password* nasabah tersebut untuk digunakan mengakses ke situs yang sebenarnya (*illegal access*) dengan maksud untuk merugikan nasabah.

Kasus-kasus di atas yang berhubungan dengan kejahatan konvensional, jika bisa dibuktikan, jelas perbuatan tersebut dapat dikualifikasikan sebagai penipuan karena dengan serangkaian perbuatan mengaku seolah-olah pemilik kartu kredit. Selain itu dapat juga dijerat dengan menggunakan pasal pencurian sebab pelaku yang berbelanja dengan menggunakan kartu kredit orang lain, mengambil secara tanpa hak sebagian atau seluruh milik orang lain dengan maksud memiliki secara melawan hukum. Akan tetapi, semua kasus tersebut memiliki kendala dalam hal pembuktian. Akibat dari transaksi melalui Internet antara lain hilangnya

sebagian atau seluruh dana yang dimiliki pemilik kartu kredit, sehingga muncul perdebatan antara pemilik kartu kredit dengan sebuah perusahaan atau sebuah lembaga bank yang akhirnya mereka baru menyadari bahwa telah terjadi suatu transaksi ilegal yang dilakukan oleh seseorang yang mempunyai data kartu kredit milik seseorang atau korban.

3. Kendala Dalam Proses Penyidikan

Dalam penanganan masalah terkait dengan *Internet Banking*, khususnya yang menyangkut penyalahgunaan kartu kredit, tampaknya ada hal yang harus diluruskan. Pada umumnya pihak *issuing bank* seringkali memiliki prasangka bahwa apabila Polri menangani kasus *credit card fraud*, maka tingkat kepercayaan konsumen, masyarakat dan pelaku usaha terhadap *issuing bank* tersebut akan turun drastis, sehingga *issuing bank* “terkesan “ hanya sedikit kooperatif. Perspektif demikian membawa implikasi pada proses penyidikan, yaitu Polri seolah-olah bekerja sendiri. Sementara pihak korban (pemilik kartu kredit dan *issuing bank*) tidak begitu diperhatikan. Akhirnya proses penyidikan menjadi tersendat dan tidak jelas penyelesaiannya.

Apabila berbagai kendala tersebut dikelompokkan, sedikitnya dapat dibedakan menjadi 2 aspek. Pertama, kendala non – teknis, yang antara lain meliputi:

- a. Korban yang dirugikan kebanyakan berada di luar negeri dan bila diminta untuk memberikan kesaksian prosesnya sangat lama (padahal sesuai ketentuan KUHAP keterangan saksi korban adalah mutlak diperlukan).
- b. Alat bukti elektronik atau *digital electronic evidence*, secara fisik mudah hilang atau dihilangkan serta masih banyak masyarakat yang belum paham tentang bagaimana cara yang efektif dan efisien dalam “mengamankan” barang bukti jenis ini.

Sedangkan hambatan teknisnya, antara lain:

- a. Diperlukan biaya yang cukup besar untuk membeli dan menyiapkan peralatan yang diperlukan dalam penyidikan kasus-kasus yang terjadi.
- b. Perlu biaya penyidikan yang tidak sedikit. Bahkan terkadang nilai kejahatan tidak sebanding dengan biaya yang dikeluarkan untuk pergi ke daerah-daerah untuk menangkap tersangka.

- c. Setelah didapatkan ISP dan *IP address* warnet atau *café net* yang digunakan tersangka/pelaku, sulit untuk “menduga” siapa saja yang pernah dan sedang menggunakan Internet tersebut untuk memesan barang yang diinginkan pelaku/ tersangka, kecuali apabila pelaku dalam bertransaksi menggunakan fasilitas Internet dan telepon rumah atau *e-mail account* berlangganan (tapi untuk yang jenis ini termasuk pelaku pemula/bodoh).
- d. Belum adanya prosedur yang tetap dan jelas dari pihak *issuing bank* yang mengeluarkan kartu kredit bila terjadi *credit card fraud*. Misalnya: bagaimana prosedur baku dan langkah-langkah yang harus dilakukan, baik oleh pemilik, otoritas *issuing bank* dan penyidik Polri bila menerima laporan awal *credit card fraud*.
- e. Sampai saat ini, belum dibangun suatu *network* yang memudah-tukan tukar informasi antara bank-*issuing bank* dengan aparat penegak hukum, sehingga penanganan kasus *credit card fraud* kurang terkoordinir.

Di sisi lain, sampai saat ini pemerintah bersama DPR (periode manapun) terkesan sangat terlambat

dalam melakukan antisipasi terhadap maraknya kejahatan yang terjadi melalui kegiatan *Internet Banking*. Bahkan dalam perkembangan terakhir, RUU Informasi dan Transaksi Elektronik yang telah “stagnan” selama 4 (empat) tahun dan seharusnya menjadi salah satu prioritas Prolegnas tahun 2005, telah dikembalikan oleh DPR kepada pemerintah dengan alasan untuk disempurnakan pada beberapa bidang. Akibatnya belum ada kepastian tentang payung hukum yang dapat secara tegas dan akurat dapat dipakai untuk melakukan penindakan terhadap pelaku tindak pidana *cyber crime*. Tidak hanya itu, saat ini juga terdapat kesan bahwa para pelaku usaha (perbankan) dan masyarakat pada umumnya kurang peduli terhadap proses penanganan kasus-kasus tindak pidana *Internet Banking*. Oleh karena itu, perlu dilakukan upaya-upaya menyeluruh dari semua pihak untuk menuju kearah yang lebih baik.

B. Solusi Alternatif

Untuk mengantisipasi berbagai permasalahan yang terkait dengan keamanan sistem informasi, maka perlu diimplementasikan suatu kebijakan dan prosedur pengamanan. Kebijakan dan prosedur tersebut harus mencakup:

1. Identifikasi sumber-sumber dan aset-aset yang akan dilindungi.
2. Analisa kemungkinan ancaman dan konsekuensinya.
3. Perkiraan biaya atau kerugian-kerugian yang dapat ditimbulkan.
4. Analisa potensi tindakan penangkal dan biayanya serta kerugian lainnya.
5. Mekanisme pengamanan yang sesuai.

Selain itu, diperlukan suatu ketentuan yang mengatur perbankan nasional yang memiliki pusat penyimpanan, pemrosesan data/informasi dan transaksi perbankan yang letaknya di luar negeri. Perlu dibentuk sebuah unit kerja khusus/ Divisi Pengamanan-Pencegahan kejahatan perbankan di dalam struktur Bank/Bank Indonesia yang fungsinya untuk melakukan penerapan kebijakan pengamanan sistem, melakukan penelitian untuk pencegahan terhadap *ancaman/kejahatan* yang sudah ada maupun yang mungkin terjadi dan melakukan tindakan *recovery* serta pemantauan transaksi perbankan selama 24 jam. Dalam rangka melakukan pengawasan terhadap perbankan, Bank Indonesia perlu melakukan audit terhadap Sistem Teknologi Informasi dan Komunikasi

yang digunakan oleh perbankan untuk setiap kurun waktu tertentu. Memperketat/mengendalikan dengan cermat akses nasabah maupun pegawai ke jaringan sistem ICT perbankan, agar seluruh pegawai perbankan mengetahui bahwa mereka pun juga dipantau. Perlu ketentuan (Peraturan atau UU) agar perbankan bertanggung jawab dengan mengganti uang nasabah yang hilang akibat kelemahan sistem pengamanan ICT perbankan, misalnya perbankan lalai meningkatkan sistem pengamanan ICT-nya, seperti halnya Regulation E di Amerika. Perlu digunakan Perangkat Lunak Komputer Deteksi untuk aktifitas rekening nasabah, agar apabila terjadi kegagalan transaksi, seperti pengambilan uang nasabah yang melampaui jumlah tertentu, dapat ditangani dengan cepat. Perlunya sosialisasi aktif dari perbankan kepada masyarakat/nasabah dan pegawai perbankan mengenai bentuk-bentuk kejahatan yang dapat terjadi dengan produk/layanan yang disediakan. Menambah persyaratan formulir identitas pada waktu pembukaan rekening baru untuk pemeriksaan pada *data base* yang menghimpun daftar orang bermasalah dengan institusi keuangan.

Meskipun hingga saat ini belum terdapat teknologi yang dapat

membuat *Internet Banking* menjadi aman, akan tetapi pihak perbankan dan pemerintah perlu mengupayakan agar penyelenggaraan *Internet Banking* yang telah ada cukup aman. Terdapat beberapa hal yang dapat dilakukan pihak perbankan untuk meningkatkan keamanan *Internet Banking*:

- Melakukan standardisasi dalam pembuatan aplikasi *Internet Banking*. Misalnya, *user interface* yang mudah dipahami, sehingga *user* dapat mengambil tindakan yang sesuai.
- Terdapat panduan bila terjadi *fraud* dalam *Internet Banking*.
- Pemberian informasi yang jelas kepada *user*. Sedangkan pihak Pemerintah dapat membebaskan masalah keamanan *Internet Banking* kepada pihak bank, sehingga bila terjadi *fraud* dalam suatu nilai tertentu, *user* dapat mengajukan klaim.

Khusus perihal beban pembuktian, perlu dipikirkan kemungkinan untuk menerapkan *omkering van bewijslast* atau pembuktian terbalik untuk kasus-kasus *cyber crime* yang sulit pembuktiannya. Hakikat dari pembuktian terbalik ini adalah terdakwa wajib membuktikan bahwa dia tidak bersalah atas dakwaan yang dituduhkan kepada terdakwa. Paling

tidak *omkering van bewijslast* ini digunakan untuk mengadili para *carder* yang berbelanja dengan menggunakan kartu kredit orang lain secara melawan hukum.

Selain pembaharuan terhadap hukum pidana materiil dan formil, juga dibutuhkan badan khusus untuk menanggulangi *cyber crime*. Dalam badan khusus tersebut termasuk penyidik khusus untuk melakukan investigasi bahkan sampai pada tahap penuntutan. Di samping itu, pelatihan perihal *cyber space* kepada aparat penegak hukum mutlak dilakukan. Sebab, seorang hakim tidak dapat menolak perkara dengan alasan tidak ada atau tidak tahu hukumnya. Sudah merupakan postulat dasar dalam ilmu hukum yang dikenal dengan adagium *ius curia novit*, artinya seorang hakim dianggap tahu akan hukumnya.

Dalam upaya peningkatan penegakan hukum terhadap pelaku *credit card fraud*, maka perlu dibuat suatu kerja sama, meningkatkan koordinasi, tukar menukar informasi secara *online* dan ditunjuk *contact person* dengan mengikutsertakan berbagai pihak. Kerja sama tersebut dapat berupa suatu gugus tugas khusus (*special task force*) yang beranggotakan asosiasi yang terkait, para *issuing bank*, dan lembaga otoritas seperti Polri dan Bank Indonesia dalam

penanganan kasus-kasus *Internet Banking*.

Sebaiknya dibuat aturan hukum yang mewajibkan setiap penyelenggara *Internet Banking* agar dalam setiap transaksi dari “siapapun” dan dari “manapun” para pihak diharuskan mencantumkan dan diminta memberikan “*digital signature* atau tanda tangan elektronik” dalam transaksi *online* tersebut. Oleh karena itu dalam pembuatan kartu kredit (disamping akan diganti dengan model chip), setiap pemilik wajib memiliki *digital signature*, sehingga minimal mengurangi risiko penyalahgunaan kartu kredit.

Selain itu, agar selaras dengan penegakan hukum yang berlangsung ditataran global, maka rekomendasi yang dihasilkan dari konferensi *Asia Pasific Fraud Advisory* juga perlu diterapkan. Dalam hal ini terutama

penting dilakukan oleh Polri dan Bank Indonesia. Hal tersebut meliputi:

- a. Mengembangkan wadah untuk melakukan hubungan informal untuk menumbuhkan hubungan formal.
- b. Pusat penyebaran ke semua partisipan.
- c. Pengkinian (*update*) data setiap bulan tentang perkembangan penanganan hukum.
- d. Program pertukaran pelatihan.
- e. Membuat format *website* antar pelaku usaha kartu kredit.
- f. Membuat pertemuan yang berkesinambungan antar penegak hukum.
- g. Melakukan tukar menukar strategi tertentu dalam mencegah atau mengantisipasi *cybercrime* di masa depan.