BAB IV
JASA-JASA PERBANKAN ELEKTRONIK ECERAN

4.1. MESIN KASIR OTOMATIS / AUTOMATED TELLER MACHINE (ATM)

4.1.5 Operasi ATM

- ATM pada umumnya digerakkan oleh sebuah kartu plastik khusus dengan sebuah PIN (Personal Identification Number/Nomor Identitas Pribadi) yang unik dan dicocokkan dengan masing-masing pengguna.
- Papan Tombol ATM biasanya menentukan jenis dan jumlah jasa-jasa yang dapat diberikan dan menawarkan beberapa/seluruh pilihan berikut :
  a. Fungsi Penarikan Uang Tunai
     - Dari sebuah rekening cek
     - Dari sebuah rekening tabungan
     - Dari sebuah rekening kartu kredit
  b. Fungsi penyetoran
     - Ke sebuah rekening cek
     - Ke sebuah rekening tabungan
     - Ke sebuah rekening lain
  c. Fungsi pemindahan uang
     - Cek ke tabungan
     - Tabungan ke cek
     - Kartu kredit ke cek
  d. Fungsi pembayaran
     - Mengurangkan dari rekening cek
     - Mengurangkan dari rekening tabungan
  e. Fungsi tambahan
     - Kesanggupan memasuki suatu rekening untuk mendapatkan saldo
- **Operasi Pengguna**
  - Masukkan kartu kedalam bacaan “MASUKKAN KARTU/INSERT CARD”
  - Masukkan nomor PIN (diberi 3 kali kesempatan)

- Memilih jenis transaksi dengan memakai papan tombol dan bisa mengubah jenis trnsaksi sebelum ”ENTER”
- Cetakan resu dibuat untuk seluruh transaksi, asli diberikan kepada nasabah melalui slot, copy karbon disimpan oleh mesin untuk pemeriksaan kasir dan untuk posting operasi.

- **Mesin Lepas Jalur (Off-line Machines)**

  Beberpa alat ATM yang kini dipakai adalah model lepas jalur, yaitu mesin yang tidak dihubungkan ke suatu komputer tetapi beroperasi secara independent dan karena itu harus membuat semua logika yang perlu untuk membaca dan menterjemahkan kartu ATM yang kemudian menulis kembali informasi ke dalam stip magnetic yang terletk di belakang kartu ATM untuk mencegah kartu dipakai lebih dai jumlah penarikan yang sah dalam jangka waktu yang telah ditentukan.

- **Mesin Pada Jalur (On-line Machines)**

  Peralatan ATM pada jalur dihubungkan langsung ke komputer sentral bank atau melalui jalur komunikasi telepon operasi on-line lebih mahal dari off-line, akan tetapi kelebihannya dalam bidang keamanan, pembaharuan arsip komputer dan pengawasan komputer untuk pengolahan transaksi bank.

  Kelebihan bagi nasabah yaitu dapat memberikan tambahan kemampuan untuk menentukan saldo rekening.

- **Kartu Plastik**

  Yaitu suatu kunci untuk sistem yang merupakan alat yang menyelenggarakan ATM dan bersama PIN mengenalkan pemkai kepada mesin. Punggung kartu memuat strip magnetik.

4.1.6. Keamanan ATM

Untuk keamanan ATM, pertama perlu diketahui berbagai cara mesin itu dapat dilanggar atau sistemnya ditipu. Cara-cara ini paling sedikit meliputi :

1. Pengesahan Gelap

Dalam setiap operasi bank, yang terpenting adalah identitas nasabah. Oleh karena itu, fungsi pertama ATM adalah mengetahui identitas pemakainya. Ini sekarang

dilakukan melalui penggunaan kartu dan PIN, dimana dianggap bahwa pemegang kedua kunci ini adalah pelanggan yang sebenarnya dan sah. Jadi sistem ini hanya sama amannya dengan bagian terlemah dari salah satu alat ini.

Pertama, bank mungkin memakai surat pos dengan 2 pengiriman terpisah untuk kartu dan untuk PIN kepada nasabah, sehingga cara ini mungkin merupakan ancaman. Berikutnya, banyak pelanggan yang mungkin tidak ingat PIN-nya dan mungkin menyimpan catatan dalam dompetnya dengan kartu secara bersamaan. Jika dompet tersebut kemudian hilang atau dicuri, penemu atau pencuri akan memperoleh kunci yang perlu untuk memasuki sistem ATM. Kemungkinan kecerobohan lain adalah pada waktu memasukkan PIN ke dalam mesin. Kebanyakan mesin memakai papan tombol vertikal, sehingga angkanya tampak oleh orang yang antri berikutnya atau orang di seberang jalan yang memakai teropong. Beberapa penjual mesin telah membuat papan tombol horizontal, sehingga mengurangi ancaman tersebut, tetapi belum menghilangkannya sama sekali, karena mesin-mesin dapat dimasuki (bugged) dengan suatu alat pendengar elektronik tersembunyi.

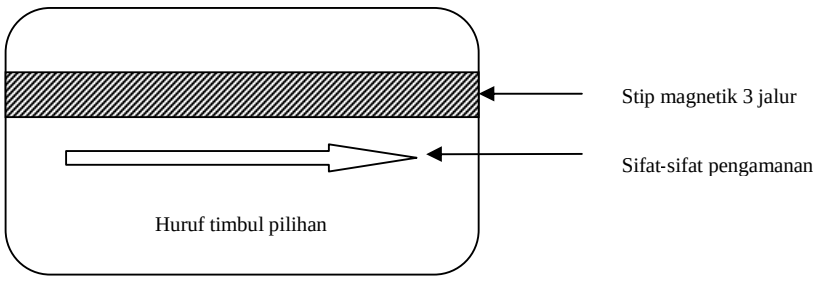
Kartu-kartu palsu merupakan ancaman pula, karena dapat dibaca dengan cepat (skimming), dan teknik-teknik yang sama memberikan cara yang akurat dan murah, dimana strip magnetik pada kartu dapat didiplikat. Ada beberapa metode untuk memindahkan data yang telah disandi (encoded) secara magnetik dari satu kartu ke kartu lain. Metodenya membutuhkan berbagai tingkat kekerampilan, dan mutu pensandian (Encoding Quality) kartu duplikat itu berkisar dari hampr sama dengan aslinya sampai pada tidak cukup baik untuk dapat diterima oleh kebanyakan terminal. Biasanya tak ada pengetahuan mengenai data yang diperlukan untuk menduplikat sebuah kartu.

Metode yang paling banyak dipakai untuk menduplikat data yang disandi secara magnetik adalah skimming (membaca cepat) dan buffer recording. Skiming adalah teknik memindahkan data dari satu strip magnetik ke strip lainnya tanpa gerakan mekanis. Operasi dasarnya adalah menempatkan sepotong pita rekaman pada strip dari kartu yang benar dan memanaskannya (apply heat) misalnya dengansebuah setruka. Berikutnya pita rekaman ditempatkan di atas strip sebuah kartu blanko dan dipanaskan lagi. Biasanya dapat dibuat beberapa kartu duplikat tanpa penurunan serius dalam mutu rekaman informasinya. Sebaliknya buffer recording (rekman penyangga) menghasilkan kartu

duplikat yang lebih tinggi kualitasnya, tetapi metode ini lebih rumit dan lebih mahal. Buffer recording membutuhkan suatu reader elektomagnetik (alat yang serupa dengan rekaman pita) dan sebuah penyimpanan buffer. Kartu ini dibaca dan datanya disimpan dalam memori buffer, dan kemudian dapat dituliskan lagi pada sebuah kartu blanko. Membuat reader electromagnetic ini membutuhkan sedikit pengetahuan.tentang elektronika dan mungkin juga mengenai format data kartu otentik.

Agar kartu-kartu lebih sulit diduplikat atau maksud-maksud gelap lainnya, beberapa penjual (vendors) menyokong penyatuan (incorporation) ciri-ciri kartu yang aman. Salah satu tekniknya adalah memakai 2 set batangan tinta magnetic yang disusun dalam pola saling menjalin dan dicetakkan pada inti sebelah dalam dari bahan plastik kartu. Kartu tersebut dapat pula mengandung tambahan penjagaan dengan bahan yang peka panas (heat-sensitive) dan peka tekanan (pressure-sensitive), sehingga setiap usaha untuk mengubah atau menduplikat batangan (bars) magnetik tersebut akan mencacatkan (invalidate) unsur-unsur keamanan yang terpadu. Hal ini kemudian akan menjadi proteksi sidik jari magnetik, dalam arti tak ada 2 kartu yang benar-benar serupa. Metode-metode lain yang juga sedang diuji adalah memasukkan isotop-isotop radioaktif yang nonlethal (tak mematikan) yang dilarutkan (diluted) ke dalam plastik kartu. Setiap kartu yang dibuat demikian akan memiliki seperangkat sifat-sifat identifikasi yang unik yang dapat dibaca mesin dan diperiksa komputer, sedangkan tetap tak mungkin diduplikat.

Berikut ini adalah gambar yang menunjukkan sebuah kartu dengan format strip magnetik dan batangan magnetik pengaman .



Ciri-ciri kartu aman ini mungkin dapat menjamin kartu tidak bisa diduplikat, karena batangan rdioaktif atau magnetik yang saling menjalin, memberikan sidik jari khusus (special finger print) yang tidak mungkin direproduksi. Akan tetapi mekanisme

ini sangat meningkatkan biaya, sedangkan fungsinya hanya melindungi kartu saja dan tidak melindungi kmponen-kmponen lain dari keseluruhan sistem. Mungkin karena alasan inilah kartu-peilikan-aman (secure property card) ini belum luas diterima umum, apalagi penyalahgunaan kartu kredit yang konvensional relative kecil.

Ada teknik-teknik lain yang sedang dikembangkan juga untuk identifikasi nasabah. Jika suatu metode terbukti secara teknis mungkin dapat diandalkan, dan efektif biaya, maka mungkin akan menggantikan kartu dan PIN. Metode-metode lain yang sedang dicoba (experimentation) meliputi identifikasi suara, identifikasi sidik jari, identifikasi pola tangan, dan identifikasi tanda tangan.

2. Pelanggaran Rantai Data

Pelanggaran terhadap rantai data merupakan ancaman yang potensial terhadap mesin-mesin on-line. Pendeknya, logika opersional bagi ATM on-line adalah menangkap data, menyampaikan data ke dan dari komputer, dan pelaksanaan instruksi (misalnya mengeluarkan uang tunai, mencetak resu, dan sebagainya) yang disampaikan kepada ATM oleh komputer. Jadi, garis penyampaian data antara ATM dan komputer dapat dilanggar dan sebuah alat dapat dimasukkan, sehingga terus-menerus memberikan insrtuksi kepada ATM untuk mengeluarkan uang tunai sampai laci (hopper) uang tunai itu kosong. Alat tersebut dikenal sebagai spoofer.

Penyadapan (taps) garis komunikasi untuk memperoleh informasi (seperti nomor rekening atau PIN) adalah ancaman potensial pula. Informasi yang diperoleh kemudian dapat dipakai pada terminal-terminal tipuan atau kartu-kartu palsu atau alat-alat lain untuk memindahkan dana ke rekening-rekening boneka (dommy).

Spoofer adalah alat elektronik transparan yang kehadirannya tak dapat dideteksi baik oleh ATM maupun komputer bank (kecuali diadaan tindakan penjagaan khusus), dan maksud utamanya adalah untuk mengelabui (defraud) bank dengan meniru komunikasi komputer ke ATM. Misalnya, jika sebuah instruksi tunggal dari komputer menyebabkan pengeluaran uang tunai oleh ATM dan ATM tidak menafsirkan lain selain melaksanakan perintah, maka penyadapan (tapping) rantai komunikasi dan penyampaian perintah pengeluaran berulang kali, hal ini akan menimbulkan kehilangan besar bagi setiap mesin. Pengamanan terhadap resiko spoofer dapat diperbaiki, pertama dengan

mengambil tindakan mengamankan garis-garis, atau kedua mempersulit menduplikat proses komunikasi antara terminal-terminal dengan komputer sentral. Penjagaan tersebut terakhir ini tidak mesti membuat sistem tersebut kebal (proof) terhadap spoofer tetapi kombinasi peningkatan biaya bagi pihak luar untuk membuat dan memasang suatu spoofer elektronik yang kompleks, ditambah dengan relative kecilnya jumlah uang tunai yang tersedia dari sebuah mesin, mungkin akan mengurangi resiko tersebut.

Terminal tipuan (imposter) adalah alat yang seperti soofer, dimasukan ke dalam garis komunikasi komputer ke ATM, dengan maksud mengelabui sistem. Dibandingkan dengan spoofer, imposter terminal ini lebh kompleks, dalam arti tidak terbatas pada komunikasi dengan ATM saja, tetapi dapat pula berkomunikasi dengan komputer. Oleh karena itu imposter terminal ini dapat memasuki (access) arsip-arsip komputer dan dipakai menggelapkan pemasukan suatu perintah transaksi keuangan yang terdapat dalam sistem kepada komputer sentral. Perlu dicatat bahwa resiko dari spoofer terhadap sistem adalah terhadap uang tunai imposer terminal dapat berupa suatu deposito yang dipegang oleh bank. Seperti halnya pada spoofer penjagaan yang potensial adalah :

- Memasang perangkat keras dan perangkat lunak (hardware dan software) untuk mendeteksi adanya suatu imposter terminal pada garis-garis komunikasi
- Lebih mempersulit pihak luar untuk menduplikat komunikasi-komunikasi antara terminal-terminal dengan komputer sentral.

1. Ketidakjujuran Pegawai

Sumber kemungkinan kehilangan lain adalah dari pegawai yang tak jujur, baik pegawai bank atau instalasi penjual, maupun manajer service. Pada umumnya, kerugian dan ketidakjujuran pegawai bank dapat ditutup oleh instansi-instansi pertanggungan (bonding agencies). Selanjutnya dapat dikatakan bahwa angka-angka statistic pencurian dalam bidang ini (baik bilangan kejahatannya maupun jumlah yang diambil) tidak terlalu berbeda dari kelas-kelas kejahatan lain oleh pegawai-pegawai bank terhadap banknya. Oleh karena itu, jika jika kurang bukti sebaliknya, maka resiko ketidakjujuran pegawai bank terhadap ATM tidak lebih besar daripada resikonya terhadap bagian-bagian lain dari bank.

Akan tetapi, resiko manajer dan pegawai pelayanan (service personnel), adalah masalah lain. Walaupun banyak dari orang-orang lain juag diasuransikan (bonded), namun tidak diketahui sejarah hubungan dan perilaku mereka, jika terbuka (expose) terhadap jumlah-jumlah yang besar.

4. Penetrasi Fisik (Pengrusakan Mesin ATM)

Usaha-usaha fisik untuk menerobos (break into) ATM harus pula dipetimbangkan. Akan tetapi jenis kejahatan ini mungkin yang terkecil resikonya bagi bank, berkat keunggulan pekerjaan rekayasa dan desain oleh penjual-penjual mesin. Ini tidak berarti bahwa mesin-mesin ini benar-benar aman dari penyalahgunaan fisik, tetapi imbalan potensialnya relatif kecil bagi usaha kejahatan dan bagi besarnya resiko tertangkap.

Berat sebuah console ATM yang biasa adalah kira-kira 650 pon. Kabinet elektronik dapat menambah berat itu 500 pon lagi, dan alat penyimpanan kas kira-kira 1600 pon – total beratnya adalah 1 ½ ton. Konstruksinya terdiri dari panel baja yang diamankan pada sebuah kerangka baja, dan kemudian dinaikkan pada dinding sebuah bangunan dan diperkuat dengan beton. Akhirnya, disamping konstruksinya yang berat itu, biasanya dipasang pula sebuah sistem alarm pengaman dan akan berbunyi jika seseorang merusakkan mesin atau mekanismenya. Pengalaman sampai sekarang menunjukkan bahwa penetrasi fisik terhadap ATM adalah bidang resiko kejahatan terkecil.

5. Resiko Off-line Khusus

Seperti telah disebutkan sebelumnya, mesin off-line yang terdapat sekarang merupakan bidang yang kemungkinan resiko pemalsuan kartunya adalah tinggi, bahkan juga lebih tinggi dari rekannya mesin on-line. Situasi khusus ini membutuhkan jaringan kerja mesin-mesin, dimana bank atau interchange (antar-tukar) dari bank-bank mempunyai beberapa ATM off-line di berbagai lokasi. Banyak bank berusaha melindungi dirinya dengan membatasi pembayaran tunai $50 per transaksi dan total jumlah transaksi sampai dua kali per hari per kartu. Selanjutnya, karena sebuah joint

accout (rekening bersama) itu mempunyai 2 kartu, maka total $200 per hari dapat sah ditarik dari rekening tersebut.