Jurnal Ilmiah Wahana Pendidikan, April 2024, 10 (8), 187-194
DOI: https://doi.org/10.5281/zenodo.11080130
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Modus Operandi Kejahatan Skimming Terhadap Nasabah Berdasarkan Perspektif Hukum Perbankan

Adia Surya Asy Syafa[1] , Imam Budi Santoso[2]

[1,2]Universitas Singaperbangsa Karawang

Received: 06 Maret 2024
Revised: 22 Maret 2024
Accepted: 30 Maret 2024

Abstract

Behind these new developments, there are different legitimate issues associated with information infringement and electronic trades in banks which, while perhaps not fittingly expected, will unquestionably hurt the bank, general society and clients. The bad behavior of taking client cash by skimming method is one of the advanced infringement (Computerized Bad behavior). In view of the skimming framework, the development is unjustly duplicating the information contained in the alluring stripe contained on Mastercards or ATM/charge cards. This suggests, it will in general be contemplated that skimming is a development associated with the offender's undertaking to unlawfully take data from the ATM/really look at card alluring tape to have control over the loss' record. This study intends to get information about monetary infringement that usage the skimming methodology and about real security for clients who are overcomers of skimming bad behavior. The investigation procedure is juridical regularizing, specifically getting and uniting and inspecting data gained from books, articles and journals and related guideline. The results procured are that bad behavior skimming is an old strategy for client cash robbery which is done by taking client data at the client's ATM with skimmer methods. Legal protection from clients who are harmed on account of the bad behavior of skimming should be possible by criminal means, specifically paying all due respects to the police and the police's commitment to catch the guilty parties. Authentic confirmation through normal guideline by means of the bank overriding the client's money resulting to making sense of the trade against the client's record.

Keywords: *Crime, Skimming, Customer Protection, Sanctions*

(*) Corresponding Author: adiasuryaas24@gmail.com

How to Cite: Syafa, A. S. A., & Santoso, I. B. (2024). Modus Operandi Kejahatan Skimming Terhadap Nasabah Berdasarkan Perspektif Hukum Perbankan. https://doi.org/10.5281/zenodo.11080130.

PENDAHULUAN

Indonesia adalah salah satu negara agraris di dunia. Kemajuan suatu bangsa berdampak pada perekonomian dan inovasi negara tersebut. Namun, dengan berjalannya waktu dan era moderenisasi, perkembangan kejahatan di ranah publin juga bertambah, terlebih di Indonesia. Seorang model melakukan kesalahan di bidang inovasi. Perbaikan kesalahan yang terkait dengan inovasi sering kali dianggap sebagai jenis kesalahan digital. Pelanggaran digital dapat terjadi tanpa memandang keberadaannya, dan dapat dilakukan oleh siapa saja. Kejahatan digital adalah kejahatan digital yang dilakukan oleh individu atau kelompok yang menyerang sistem keamanan komputer atau informasi di komputer. Perbuatan salah tersebut dilakukan dengan niat yang berbeda-beda, mulai dari sombong hingga pelanggaran yang dapat merugikan.

Seiring berjalannya waktu dan inovasi menjadi lebih maju, kejahatan digital telah berkembang menjadi berbagai jenis kejahatan baru dengan cara-cara baru

yang biasa dalam melakukan sesuatu. Jenis-jenis kejahatan digital terus bermunculan, mulai dari yang biasa disebut, misalnya hacking, cracking, carding hingga yang lebih khusus lagi, misalnya probe (berusaha mendekati sistem); scan (probe dengan jumlah besar); account compromise (pemanfaatan catatan secara melawan hukum); root split the Difference (akun membagi selisihnya dengan penghargaan untuk gatecrasher); keuangan administrasi atau DoS (membuat organisasi menjadi kacau karena dibanjiri traffic); penyalahgunaan nama spasi, dan sebagainya.

Tugas inovasi data di segala bidang kehidupan manusia sangatlah penting, mengingat dunia perbankan. Kemajuan kerangka keuangan tidak dapat dipisahkan dari tugas inovasi data. Semakin berkembang dan kompleksnya kantor yang dilakukan oleh bank untuk bekerja sama dengan administrasi, semakin berbeda dan memiliki tingkat kesuliatan penerimaan inovasi di sebuah bank. Selain bekerja dengan tugas-tugas internal organisasi, perangkat mekanis juga dimaksudkan untuk bekerja dengan administrasi kepada nasabah bank. Karena hampir setiap barang yang diajukan kepada klien tidak sepenuhnya berbeda, maka pertentangan dalam dunia keuangan adalah cara menyediakan barang yang sederhana dan cepat. Kegiatan perbankan dengan pertukaran elektronik (e-banking) melalui mesin ATM, phone banking (telepon perbankan) dan organisasi web (Web banking), adalah beberapa contoh administrasi pertukaran perbankan yang menggunakan inovasi data. Menurut sudut pandang keamanan, pemanfaatan inovasi dapat memberikan informasi dan pertukaran asuransi keamanan.

Kejahatan perampokan aset melalui *skimmer* merupakan perbuatan kezaliman yang luar biasa. Dilihat dari banyaknya pelanggaran yang terjadi di masyarakat, khususnya korban kejahatan skimmer, pelanggaran khususnya perampokan dukungan nasabah bank melalui perangkat skimmer telah menimbulkan perspektif negatif bagi perbankan secara umum dan juga masyarakat. Hal ini karena keamanan dan kenyamanan nasabah serta masyarakat menjadi kendala atau penghambat dalam melakukan penyalahgunaan subsidi nasabah bank melalui perangkat skimmer. Melalui melakukan berbagai penilaian secara konsisten, misalnya membenahi atau mengembangkan lebih lanjut kerangka keamanan bank sehingga menghasilkan kerangka keamanan yang baik dan baik. Polisi dapat lebih siap untuk menangani setiap kejadian perampokan aset melalui skimmer dan polisi dapat meneliti dan mencari bukti yang ada dengan lebih efektif.

Berdasarkan penyataan permasalahan yang ada, rumusan permasalahan untuk peneltian ini adalah sebagai berikut:

1. Bagaimana kejahatan permbobolan uang nasabah dengan menggunakan metode skimming dilihat dari persfektif hukum?
2. Bagaimana cara kerja skimmer dalam melakukan kejahatan dalam perbankan?
3. Bagaimana pencegahan serta pelindungan hukum pada nasabah yang menjadi korban aktivitas pembobolan rekening nasabah dengan metode skimming dilihat dari persfektif hukum?

Dengan demikian, dari rumusan permasalahan yang terjadi, tujuan penelitian ini dilakukan adalah sebagai berikut:

1. Untuk menganalisis tindak kejahatan skimming
2. Untuk mengetahui cara kerja skimmer dalam melakukan kejahatan dalam perbankan

3. Untuk mengetahui cara pencegahan dan perlindungan hukum pada nasabah yang menjadi korban kejahatan skimming

METODE PENELITIAN

Kejahatan perbankan yang menggunakan inovasi data sangatlah beragam, namun dalam penelitian ini penulis hanya menyoroti analisis kesalahan pengambilan uang nasabah yang dilakukan oleh oknum-oknum nakal yang menggunakan teknik Skimming dan melihat keamanan sah bagi nasabah yang menjadi penyintas pelanggaran dengan menggunakan strategi skimming. .

Dengan demikian, penelitian ini menerapkan pendekatan penelitian yuridis normatif yang termasuk dalam kategori penelitian normatif yang memanfaatkan informasi sekunder. Informasi yang diperoleh kemudian diproses dan dianalisa guna menjawab permasalahan yang terkait.

HASIL DAN PEMBAHASAN

Skimming Menurut Perspektif Hukum Perbankan

Menurut penelitian yang dilakukan oleh Kristian, istilah-istilah pelanggaran perbankan dihimpun ke dalam dua kategori, kumpulan pokoknya merupakan kumpulan demonstrasi kriminal di bidang keuangan, yang maknanya setara dengan pentingnya istilah pelanggaran di bidang keuangan, demonstrasi kriminal di bidang perbankan atau kesalahan terhadap perbankan. Kategori selanjutnya adalah perbankan yang salah, yang maknanya mencakup pengertian istilah perbankan yang salah. Seperti yang telah dijelaskan di atas, istilah tindak pidana perbankan harus dipahami, dalam konteks istilah tindak pidana di sektor keuangan. Tindakan salah dalam perbankan adalah tindakan yang melanggar aturan perbankan yang telah ditetapkan, dan dapat dikenakan sanksi pidana berdasarkan Peraturan Keuangan (Peraturan Nomor 7 Tahun 161 Tahun 1992 yang telah diubah oleh Peraturan Nomor 10 Tahun 1998 tentang Perbankan).

Kejahatan pidana di sektor keuangan mengacu pada tindakan criminal yang terkait dengan operasi pokok suatu bank. Tindakan ini dapat disangkal karena melanggar undang-undang keuangan atau regulasi-regulasi yang berhubungan dengan industry perbankan.

Dalam konteks yang telah dijelaskan sebelumnya, aktivitas kejahatan dalam perbankan merupakan bentuk tindak pidana yang terkait dengan aspek keuangan, khususnya pelanggaran yang memiliki motivasi finansial. Tindak pidana ini umumnya dilakukan oleh individu yang memiliki pemahaman logika dan menduduki posisi yang penting dalam masyarakat, terutama dalam konteks pekerjaan dan peran mereka di mata masyarakat.

Dalam modus operandi "pencurian bank" melalui skimming, komponen untuk mengambil informasi klien disimpan pada strip yang menarik pada kartu ATM dan dikirim dari jarak jauh. Teknik pembobolan informasi ini dilakukan dalam beberapa tahap, yakni terlebih dahulu pelaku memasang alat skimmer (penangkap informasi elektronik) di slot mesin ATM, lalu pelaku memasang kamera pengintai untuk melihat data nasabah. Selain itu, pelaku tindak kejahatan ini melakukan cetakan ATM guna memberikan pesan bahwa uang yang ada di ATM sudah tidak ada, padahal sebelunya nasabah sudah menginput PIN dan kartu.

Sesudah para pelaku memperoleh informasi klien. Mereka membuat Salinan informasi ke dalam kartu palsu. Terkadang, pelaku tidak perlu lagi menggunakan kamera tersembunyi, tetapi cukup melihat informasi tersebut dari belakang bahu klie. Seiring berjalannya waktu, pelaku yang melakukan *skmming* tidak perlu lagi mengandalkan kamera tersembunyi atau pengintipan dari belakang bahu klien, melainkan mereka menggunakan keypad palsu di mesin ATM untuk mencatat PIN. Pembobotan bank dapat dibedakan menjadi dua macam, yaitu:

1. *Error Omission*

Untuk lebih spesifiknya adalah "representasi bank yang salah" dengan mengabaikan kerangka atau sistem yang tidak terlibat atau tidak mencapai sesuatu yang seharusnya diselesaikan. Teknik yang tidak terlibat di sini menyinggung sistem dan standar pembukuan, khususnya unsur tugas administratif, pencatatan pertukaran dan penjurnalan. Pelanggaran ini mempunyai bentuk standar yang jelas dan terlebih lagi kewenangan yang jelas, pada umumnya kewenangan manajerial.

2. *Error Commission*

Lebih spesifiknya adalah "perampokan bank" yang berhasil diselesaikan melalui kegiatan di luar basis, namun karena tidak disusun dalam struktur dan kerangka, maka dilakukanlah. Pelanggaran ini erat kaitannya dengan keaslian orang-orang di bank sebenarnya. Pelanggaran-pelanggaran ini akan bergantung pada normalisasi persetujuan, namun umumnya ditujukan kode etik.

Metode *skmming* bisa diterapkan dengan mengajak seseorang untuk berperan sebagai pelayan restoran, lalu memberikan kepada mereka alat perekam data (*skimmer*) yang berukuran kecil. Alat perekam data ini digunakan untuk menggesek kartu saat proses pembayaran dengan kartu, aktivitas ini mengkolaborasikan mungkin hanya berlangsung beberapa detik dan umumnya terjadi ketika pemilik kartu tidak mengawasi, sehingga sulit untuk mendeteksi tindakan skimming. Selain digunakan dalam skimming pada individu, skimmer juga sering ditemukan pada mesin ATM. Penggunaan *skimmer* pada mesin ATM dilakukan agar mesin terlihat seolah-olah menjadi komponen penting yang perlu digunakan oleh nasabah, yang pada akhirnya menipu mereka untuk memasukkan kartu ATM.

Dalam praktek “Pencurian bank” pada umumnya melibatkan pihak-pihak yang berada di dalam bank, karena kelompok tersebut mempunyai informasi dan akses mengenai seluk beluk, komponen dan sistem keamanan bank yang ingin mereka hancurkan. Bagaimanapun juga, kontribusi individu pada bank tentu saja bukan merupakan prasyarat mutlak terjadinya aktivitas "perampokan bank". Delapan kasus "perampokan bank" yang digambarkan di atas menunjukkan beragamnya pelaku pencurian. Biasanya, pelaku "perampokan bank" dapat melakukan tiga cara, khususnya:

1. Pembobolan bank yang dilakukan oleh internal bank
2. Pembobolan bank yang dilakukan oleh external bank
3. Pembobolan bank yang dilakukan antara internal dan external bank.

Cara Kerja *Skimmer* Dalam Melakukan Kejahatan Dalam Perbankan

Skimming sebagai tindakan kejahatan menyasar mesin ATM dengan cara mengendalikannya untuk mendapatkan informasi atau data mengenai catatan nasabah atau rekening investasi yang disimpan pada strip kartu kredit. Terlepas dari kenyataan bahwa bank telah memperkenalkan perangkat keras anti skimming, masih ada prosedur yang digunakan oleh skimmer untuk mengambil cadangan

klien. Berikut beberapa prosedur umum yang digunakan untuk mengambil informasi nasabah dari penggunaan kartu cek di mesin ATM:

1. Memasang *deep insert skimmer* di mesin ATM

Gadget atau perangkat ramping dimasukkan ke dalam bukaan kartu di mesin ATM. Ukurannya yang ramping mampu 'mengakali' kemampuan alat counter skimmer yang dipasang di mesin ATM, sehingga kehadiran skimmer ini tidak diketahui. Perangkat skimmer tambahan yang mendalam mampu merekam informasi kartu dan kemudian menyimpannya di drive kecil. Cara kerja alat skimmer suplemen mendalam adalah dengan menangkap informasi pada kartu ATM dari strip menarik di bagian belakang kartu. Oleh karena itu, kartu ATM yang kerangka keamanannya hanya untuk keperluan pita menarik rentan terhadap skimming. Untuk mengatasi hal tersebut, bank telah menyiapkan highlight keamanan kartu ATM dengan gadget chip. Jika dibandingkan dengan pita perekat yang menarik, chip dianggap lebih aman untuk menghindari kesalahan.

2. Memasang *fake card reader* di pusat perbelanjaan

Transakssi yang menggunakan biaya atau Visa umumnya tidak dilindungi, tidak ada jaminan keamanan bahkan dari bank yang bertanggung jawab. Oleh karena itu, klien harus selalu siap dan berhati-hati saat melakukan penukaran menggunakan charge atau Mastercard di mana saja, apalagi di mall. Alasan sederhana dan fungsional sebagian besar menjadi alasan melibatkan kartu untuk transaksi. Namun perlu diketahui dan dipahami bahwa kegiatan skimming tidak hanya menyasar mesin ATM saja, namun juga mesin EDC (Electronic Information Catch) yang biasa digunakan pada pegawai plaza retail. Tanpa disadari, saat melakukan penukaran, mesin EDC yang digunakan telah dilengkapi dengan skimmer sebagai pembaca kartu palsu sehingga seluruh informasi atau data yang disimpan pada tagihan atau Visa dapat diambil dan kemudian dikloning ke dalam kartu yang belum terisi.

3. Memasang lubang kartu ATM palsu

Ada banyak cara yang digunakan skimmer untuk mengambil uang cadangan nasabah bank. Salah satu caranya adalah dengan memperkenalkan pembukaan kartu ATM palsu. Tujuannya tentu saja untuk mendapatkan data tagihan nasabah atau Visa yang ditempelkan pada ruang kartu di mesin ATM. Lubang kartu ATM sebagian besar memiliki pengguna kartu yang diperkenalkan di dalamnya. Lubang kartu ATM pertama umumnya diperkenalkan sebagai satu kesatuan dengan mesin ATM sehingga sulit untuk dibongkar. Rata-rata, pembukaan kartu ATM palsu umumnya akan lebih besar karena diperkenalkan mencakup pembukaan ATM pertama. Selain itu, sangat mudah untuk dimusnahkan atau dihilangkan, karena tidak terhubung dengan mesin ATM.

Pada mulanya skimmer berukuran besar dan sepertinya tidak diperlukan untuk mesin ATM, namun semakin berkembangnya teknologi, skimmer tersebut memiliki ukuran yang kecil dan bekerja hanya dengan memanfaatkan baterai, umumnya diperkenalkan dimana kartu ATM ditancapkan menggunakan dua sisi penutup dengan tujuan agar kartu ATM nasabah dapat dimasukkan melalui skimmer pada saat nasabah perlu menyelesaikan transaksi. Informasi yang diperoleh melalui skimmer kemudian ditempelkan ke dalam kartu palsu yang juga memiliki strip menarik sehingga dapat digunakan dengan baik di mesin ATM seperti halnya nasabah yang menggunakan kartu ATM.

Berbeda dari *malware* dan *phising* modern yang dengan cepat mengambil semua informasi nasabah, karena skimming, prosedur ini juga mencakup teknik menyeluruh untuk mendapatkan PIN nasabah sehingga pelaku skimming dapat memasuki mesin kartu ATM dengan menggunakan informasi nasabah. Mendapatkan PIN klien seharusnya dapat dilakukan dengan beberapa sistem, termasuk sistem yang paling mudah dengan melihat kapan klien memasukkan PIN dari belakangnya. Selain itu, strategi ini juga mencakup pengenalan kamera yang merekam perkembangan jari nasabah saat memasukkan PIN, atau lebih baru lagi dengan memasang keypad palsu di mesin ATM. Keypad palsu ini dihadirkan oleh pelaku dengan tujuan dapat merekam PIN klien dengan andal ketika klien menekan tombolnya. Setelah mengetahui informasi klien pelaku yang dimasukkan ke dalam kartu palsu dan PIN klien, mereka dapat melakukan perdagangan menggunakan kartu ATM, termasuk penarikan tunai, transfer ditahan, dan porsi tagihan.

Pencegahan Yang Dilakukan dan Perlindungan Hukum Nasabah

Berikut merupakan beberapa cara melakukan pencegahan Teknik *skimming* pada kartu ATM:

1. Tutup PIN ATM dengan tangan saat memasukkannya.
2. Periksa mesin ATM yang akan digunakan, terutama pada bagian tombol ATM.
3. Disarankan untuk menggunakan ATM yang memiliki keramaian atau pengawasan ketat.
4. Rutin merubah PIN ATM
5. Ganti kartu ATM dengan berbasis chip. Modus skimming umumnya mencuri data dari pita magnetic kartu. Dengan menggunakan kartu berbasis chip, Anda akan mendapatkan perlindungan ekstra karena data yang tersimpan dalam chip terenkripsi dan tidak dapat dibaca saat kartu melewati skimmer.

Informasi nasabah, termasuk informasi data yang berhubungan dengan pribadi nasabah, merupakan laporan dan data yang penting dan tentunya harus dirahasiakan oleh Bank. Informasi nasabah tidak boleh disebarkan oleh bank ke pada pihak luar kecuali hal ini menjadi suatu persoalan. Informasi nasabah perbankan seperti PIN (Individual Recognizable Proof Number), nomor Visa dan sebagainya harus dirahasiakan oleh bank. Pelanggaran perlindungan klien oleh bank dapat ditangkap secara pidana. Apabila terjadi kesalahan, termasuk menyalin kartu ATM nasabah, tentu akan membawa malapetaka bagi nasabah. Kesalahan ini akan mengakibatkan penurunan saldo uang tunai nasabah di bank, tentunya perlindungan hukum harus disediakan bagi klien yang menjadi korban tindak pidana *skimming* ini. Perlindungan hukum yang sah bagi klien yang terdampak oleh tindak pidana *skimming* dapat menjamin dengan mematuhi peraturan pidana dan umum.

Aktivitas skimming di atas mencakup aktivitas melanggar hukum yang memasuki komputer atau kerangka data orang lain untuk tujuan yang melanggar hukum, khususnya mengambil informasi data individu yang disimpan di komputer atau kerangka tersebut. Kegiatan ini mengingat pelanggaran peraturan di bidang pertukaran data dan elektronik yang menghalangi siapa pun dengan sengaja dan tanpa persetujuan atau saluran yang sah untuk mengakses komputer atau kerangka elektronik dalam kapasitas apa pun, dengan niat penuh untuk memperoleh data elektronik dan laporan elektronik, sebagai diarahkan pada Pasal 30 ayat 2 Peraturan

Nomor 19 Tahun 2016 yang mengatur perubahan atas Peraturan Nomor 11 Tahun 2008 tentang pertukaran dan data elektronik yang disebut juga Peraturan ITE.

Pasal 30 ayat 2 Peraturan ITE secara lebih luas menyatakan "Setiap orang dengan sengaja dan tanpa persetujuan atau melanggar hukum mengakses komputer atau kemungkinan kerangka elektronik dengan menggunakan strategi berbeda dengan tujuan penuh untuk mendapatkan data elektronik serta catatan elektronik."

Setiap tindakan dapat dikenai hukuman jika memenuhi elemen-elemen kejahatan yang tercantum dalam pasal yang relevan. Dalam konteks Pasal 30 ayat 2 Undang-Undang ITE, unsur-unsur kejahatannya meliputi:

1. Unsur kesalahan, yang berarti dilakukan dengan sengaja
2. Unsur melawan hukum, artinya tanpa izin atau melawan hukum.
3. Unsur perbuatan, yaitu mengakses dengan berbagai cara.
4. Unsur obyek, yang mencakup computer dan/atau sistem elektronik.
5. Tujuan, yang adalah untuk memperoleh informasi elektronik dan/atau dokumen elektronik.

Sanksi pasal 30 ayat 2 Peraturan Pertukaran Data dan Elektronik (ITE) tertuang dalam pasal 46 ayat 2 Peraturan serupa yang mensyaratkan "Setiap orang yang memenuhi komponen sebagaimana direncanakan dalam Pasal 30 ayat (2) akan diberikan sanksi berupa sanksi penahanan paling ekstrim selama 7 (tujuh) tahun serta denda terbesar sebesar Rp700.000.000,00 (700.000.000 rupiah).

KESIMPULAN

Skimming adalah aktivitas pengambilan data kartu kredit atau tagihan dengan cara mereplikasi data secara tidak sah pada strip kartu kredit atau cek secara ilegal. Strip magnetik ini adalah tempat penyimpanan data tentang kartu. Dalam metodologi biasa disebut "perampokan bank" melalui Skimming, penyelesaiannya dilakukan dengan mengambil informasi klien yang disimpan pada strip menarik pada kartu ATM dan dikirim dari jarak jauh. Proses perampokan informasi ini melibatkan beberapa langkah, dimulai dengan langkah pertama di mana pelaku memasang alat *skimmer* (perangkap informasi elektronik) pada slot mesin ATM. Selanjutnya, pelaku memasang kamera tersembunyi untuk merekam Gerakan jari nasabah saat mereka memasukkan PIN ATM. Seringkali, pelaku juga menggunakan penutup PIN, seperti kotak selebaran, untuk menyamarkan aktivitas mereka. Selain itu, mereka mencetak pesan palsu pada mesin ATM yang membuat nasabah percaya bahwa mesin tersebut kosong, meskipun sebenarnya sebelumnya pelaku telah mencuri PIN dan kartu ATM. Kemudian, setelah pelaku mendapatkan informasi klien, pelaku menggandakan informasi tersebut ke dalam kartu palsu. Demonstrasi skimming di atas mencakup demonstrasi mengakses komputer orang lain dan juga kerangka data dengan cara yang melanggar hukum dengan maksud untuk secara salah memulihkan informasi individu yang terdapat dalam komputer atau kerangka data potensial. Kegiatan ini termasuk tindak pidana karena terjadi pelanggaran transaksi data menggunakan perangkat elektronik yang menghalangi setiap individu untuk dengan sengaja dan tanpa hak atau melanggar hukum mengakses computer dan sistem elektronik dalam kapasitas yang ditentukan untuk mengambil data elektronik dan catatan elektronik sesuai dengan ketentuan dalam Pasal 30 ayat 2 Undang-Undang. Hal ini diatur dalam peraturan Nomor 19 Tahun 2016 yang mengubah peraturan Nomor 11 Tahun 2008 mengenai Pertukaran Data

Elektronik atau yang lebih dikenal dengan peraturan ITE. Apabila terjadi kesalahan, termasuk tindakan menyalin kartu ATM nasabah, tentu saja akan menimbulkan bencana bagi nasabah. Kesalahan ini akan mengakibatkan kekurangan uang tunai bagi nasabah bank. Oleh karena itu, sangat penting untuk memiliki perlindungan hukum bagi klien yang menjadi korban *skimming.* Keamanan yang sah bagi *klien* yang menjadi korban tindakan *skimming* dapat dicapai dengan mematuhi hukum pidana dan peraturan umum.

DAFTAR PUSTAKA

Hermansyah. (2009). Hukum Perbankan Nasional Indonesia. Dalam *Hukum Perbankan Nasional* (hal. 160). Jakarta.

Humris, R. (2015). Memahami Motif & Mengantisipasi Penyalahgunaan Wewenang. Dalam *Memahami Motif & Mengantisipasi Penyalahgunaan Wewenang* (hal. 74). Jakarta: Gramedia Pustaka Utama.

Indonesia, T. P.-U. (2006). *Urgensi Cyberlaw di Indonesia Dalam Rangka Penanganan Cybercrime di Sektor Perbankan.* Jakarta.

Kristian, & Gunawa, Y. (2013). Tindak Pidana Perbankan. *Nuansa Aulia*.

Kusuma, M. J. (2012). Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank Terhadap Tindak Kejahatan ITE di Bidang Perbankan. *Nusa Media*.

Sugiharto, T. (2010). Tips ATM Anti Bobol: Mengenal Modus-modus Kejahatan Lewat ATM dan Tips Cerdik Menghindarinya. Dalam T. Sugiharto, *Tips ATM Anti Bobol: Mengenal Modus-modus Kejahatan Lewat ATM dan Tips Cerdik Menghindarinya* (hal. 88-141).