Pembuktian dalam Kejahatan Carding dan Upaya Pihak Perbankan dalam Melakukan Penanganan terhadap Data Nasabah Kartu Kredit menurut Hukum Pidana Positif di Indonesia

Aldo Fuqaha Alfatih*, Dian Alan Setiawan

Prodi Ilmu Hukum, Fakultas Hukum, Universitas Islam Bandung, Indonesia.

*dofuqaha@gmail.com, dianalan.setia@yahoo.com

Abstract. Carding is a serious problem in Indonesia, related to crimes using credit cards and theft of personal data via the internet. This crime can be subject to articles from several laws and regulations to ensnare the perpetrator. However, proof in carding crimes becomes difficult, especially related to information technology. This research aims to explore the way of proof in carding crimes according to positive criminal law in Indonesia. The research method used is descriptive qualitative with analysis of primary, secondary, and tertiary legal materials. The results show the difficulty in obtaining valid evidence in accordance with Article 184 of the Criminal Procedure Code because it requires human resources and good forensic computer equipment. Obstacles also arise because many witnesses, suspects, and victims are outside the jurisdiction of Indonesian law. Banking efforts to protect credit card customer data are in accordance with Article 40 paragraph (1) of Law No. 10 of 1998, which requires banks to maintain the confidentiality of customer information. In the context of cyber resilience, banks are further regulated by the Financial Services Authority Circular Letter Number 29/Seojk.03/2022 on Cyber Resilience and Security for Commercial Banks. These efforts reflect the banking response to the increasingly complex challenges of carding crimes in the digital era.

Keywords: *Carding, Digital Banking Transactions, Credit Card Data Theft*.

Abstrak. Carding menjadi masalah serius di Indonesia, terkait dengan kejahatan menggunakan kartu kredit dan pencurian data pribadi melalui internet. Kejahatan ini dapat dikenakan Pasal-pasal dari beberapa peraturan perundang-undangan untuk menjerat pelaku. Namun, pembuktian dalam kejahatan carding menjadi sulit, terutama terkait dengan teknologi informasi. Penelitian ini bertujuan menggali cara pembuktian dalam kejahatan carding menurut hukum pidana positif di Indonesia. Metode penelitian yang digunakan adalah deskriptif kualitatif dengan analisis bahan hukum primer, sekunder, dan tersier.Hasil penelitian menunjukkan kesulitan dalam mendapatkan bukti sah sesuai dengan Pasal 184 KUHAP karena memerlukan sumber daya manusia dan peralatan komputer forensik yang baik. Hambatan juga muncul karena banyak saksi, tersangka, dan korban berada di luar yurisdiksi hukum Indonesia. Upaya perbankan untuk melindungi data nasabah kartu kredit sesuai dengan Pasal 40 ayat (1) UU No. 10 Tahun 1998, yang mewajibkan bank menjaga kerahasiaan informasi nasabah. Dalam konteks ketahanan siber, bank diatur lebih lanjut oleh Surat Edaran Otoritas Jasa Keuangan Nomor 29/Seojk.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum. Upaya ini mencerminkan respons perbankan terhadap tantangan kejahatan carding yang semakin kompleks di era digital.

Kata Kunci: *Carding, Transaksi Perbankan Digital, Pencurian Data Kartu Kredit.*

Corresponding Author
Email: dianalan.setia@yahoo.com

A. Pendahuluan

Perkembangan teknologi banyak kaitannya dengan gaya hidup manusia dan banyak keuntungannya akan tetapi ada juga kerugiannya. Penggunaan komputer, telekomunikasi dan teknologi informasi telah memfasilitasi pertumbuhan transaksi Internet di seluruh dunia. Pelaku bisnis di Indonesia dan global semakin banyak yang menggunakan perangkat Internet sebagai sarana transaksi bisnis. Pada saat yang sama, transaksi elektronik atau online di berbagai bidang semakin meningkat, membawa serta berbagai istilah yang berbeda, termasuk perbankan elektronik. Internet Banking atau perbankan elektronik adalah salah satu layanan Bank yang memungkinkan nasabah memperoleh informasi, berkomunikasi dan melakukan transaksi perbankan melalui Internet. Saat melakukan pembelian online melalui electronic banking, transaksi hanya boleh dilakukan dengan menggunakan kartu kredit yang diterbitkan oleh penerbit kartu kredit. Carding saat ini menjadi masalah yang sangat pelik di Indonesia, carding merupakan kejahatan yang berhubungan dengan penggunaan kartu kredit. Motif kejahatan ini adalah melakukan pembelian dengan menggunakan identitas dan nomor telepon orang lain, dengan metode pencurian data pribadi orang lain melalui Internet. Hal ini tentu melanggar Pasal 35 Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Namun dalam hal pembuktian kejahatan carding ini penegak hukum di Indonesia masih kesulitan untuk membuktikannya karena Carding merupakan kejahatan yang dilakukan seseorang dengan keahlian khusus, karena kejahatan tindak pidana carding merupakan kejahatan yang dimana pelaku kejahatan ini menggunakan kecanggihan teknologi sehingga dalam menangani kasus seperti ini kepolisian Indonesia mengalami kesulitan dan hambatan dalam mencari alat bukti atau pelaku. Dalam Pasal 184 ayat (1) mengatur mengenai alat bukti, dalam pasal ini tidak menyebutkan mengenai alat bukti kejahatan elektronik sehingga dapat menimbulkan berbagai kemungkinkan pada saat melakukan penyelidikan, seperti mengenai alat bukti digital yang masih butuh keahlian khusus untuk mengetahui keaslian dari alat bukti tersebut, dengan melihat kasus carding ini dilakukan oleh pelaku yang ahli dalam bidang teknologi tidak menutup kemungkinan bahwa pelaku dapat menghilagkan alat bukti tersbut. Selain itu dalam melakukan penyelidikan polisi mengalami kesulitan dalam mencari keterangan saksi seperti korban dari kejahatan carding yang sebagian besar korbannya merupakan warga negara asing sehingga untuk memintai keterangan dibutuhkan prosedur tertentu karena menyangkut masalah yuridiksi negara lain. Dalam sistem peradilan hukum acara pidana pembuktian dalam suatu perkara adalah hal yang sangat penting. Hukum positif mengharuskan adanya alat bukti, saksi, petunjuk, keterangan ahli serta terdakwa dalam pembuktian. Sedangkan dalam hal kejahatan terkait dengan carding ini sangat sulit untuk di buktikan. Dengan berbagai hambatan dalam pembuktian tindak pidana carding maka perlu adanya upaya pihak perbankan dalam melakukan pengamanan terhadap data nasabah kartu kredit agar dapat meminimalisir kejahatan tindak pidana carding tersebut. Para nasabah mempunyai hak untuk mendapatkan kerahasiaan dan keamanan data pribadi. Pemerintah menerapkan prinsip kerahasiaan bank yang diatur melalui Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Prinsip kerahasiaan bank ini dimana mengatur mengenai bank yang berkewajiban menjaga dan merahasiakan informasi keuangan milik nasabahnya dari pihak manapun. Perlindungan hukum terhadap data pribadi merupakan kebutuhan yang penting bagi setiap individu, dan tanggung jawab bagi negara untuk melindungi hak-hak dasar tersebut sebagai lembaga yang membuat kebijakan, hal ini terdapat pada bagian menimbang Undang-Undang No 22 Tahun 2022 tentang Perlindungan Data Pribadi.

Berdasarkan latar belakang yang telah diuraikan, maka perumusan masalah dalam penelitian ini sebagai berikut: “Bagaimana pembuktian dalam kejahatan carding dan upaya perbankan untuk melakukan pengamanan terhadap data nasabah kartu kredit menurut peraturan perundang-undangan”. Selanjutnya, tujuan dalam penelitian ini diuraikan dalam pokok-pokok sbb.

1. Untuk Mengetahui Pembuktian Dalam Kejahatan Carding Menurut Hukum Pidana Postitif di Indonesia
2. Untuk Mengetahui Upaya Perbankan dalam kejahatan carding untuk melakukan pengamanan Terhadap Data Nasabah Kartu Kredit Menurut Peraturan Perundang-

Undangan

B. Metodologi Penelitian

Penelitian ini menggunakan metode deskriptif kualitatif, yakni analisis terhadap bahan hukum primer, sekunder, dan tersier. Meliputi klasifikasi bahan hukum sesuai dengan permasalahan dan topik penelitian kemudian di sesuaikan dengan ketentuan hukum, dimana hasil akhir analisis adalah dalam bentuk narasi berupa pengambilan kesimpulan secara deduktif.

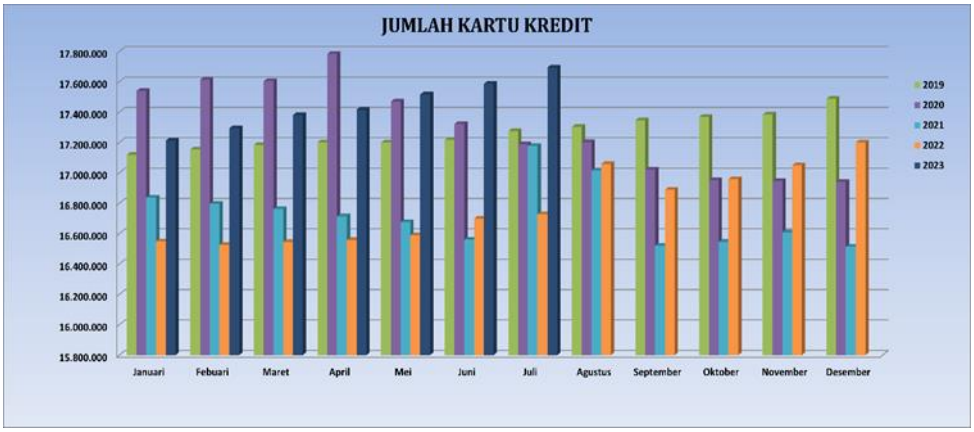
Dalam metode pendekatan ini penelitian akan di awali dengan menganalisis pasal-pasal Kitab Undang-Undang Hukum Acara Pidana yang mengatur mengenai pembuktian dan alat bukti, dikaitkan dengan penanganan perkara cybercrime (carding) yang sudah ada serta perundang-undangan lain yang mencakup mengenai permasalahan mengenai penanganan data nasabah kartu kredit oleh pihak perbankan.

C. Hasil Penelitian dan Pembahasan

Hambatan-Hambatan Kejahatan Carding

Perkembangan teknologi khususnya dalam bidang digital mengalami perkembangan yang sangat pesat, perkembangan itu menghadirkan teknologi yang bisa membantu aktivitas transaksi keuangan dalam hal ini bank. Seperti melakukan transaksi pengiriman uang sekarang tidak harus pergi ke atm atau menggunakan cara konvensional, namun dengan kehadiran jaringan internet meberikan kemudahan pada nasabah bank untuk melakukan transaksi keuangan dengan cara internet banking atau m-banking, sehingga bisa dilakukan dengan mengoprasikan aplikasi m-banking yang ada di smart phone nasabah bank.

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 Asosiasi Kartu Kredit Indoneisa (Indonesia Credit Card Association) tahun 2023 jumlah pemegang kartu kredit di Indonesia sudah mencapai lebih dari 17 juta kartu yang beredar di Indonesia.



Gambar 1. Jumlah Kartu kredit

Jumlah pemegang kartu kredit selama kurun waktu 5 tahun terakhir di Indonesia menunjukkan tren yang relatif naik turun seiring dengan kemajuan industri perbankan. Dengan banyaknya jumlah pemegang kartu kredit di Indonesia menyebabkan perkembangan teknologi dalam bidang elektronik banking ini membawa potensi kejahatan baru yang lebih besar. Kejahatan ini adalah kejahatan carding melalui jaringan internet.

Dalam konteks beberapa jenis kejahatan dunia maya di Indonesia, salah satu bentuknya adalah carding. Carding merupakan suatu tindakan penipuan yang terkait dengan kartu kredit, di mana pelaku dapat memperoleh informasi nomor kartu kredit yang masih aktif dan menggunakannya untuk pembelian barang secara online. Dengan demikian, pelaku dapat membuat tagihan atas pembelian tersebut dialamatkan kepada pemilik kartu kredit yang sebenarnya. Orang yang melakukan carding disebut sebagai carder. Dalam bahasa formal atau

hukum, istilah carding masuk dalam kategori credit/debit card fraud atau penipuan menggunakan kartu kredit/kartu debit.

Pengaturan mengenai tindak pidana carding diuraikan sesuai dengan modus operandi kejahatan tersebut dalam Undang-Undang ITE. Hal ini dijelaskan sebagai lex specialis, yang dianggap sebagai keharusan yang mendesak. Ini disebabkan oleh ketidakmampuan menyejajarkan tindak pidana carding dengan kejahatan konvensional lainnya yang umumnya terjadi di dunia nyata. Dalam ruang siber, kegiatan ini bersifat virtual, tetapi dampaknya sangat nyata. Penetapan undang-undang di luar KUHP, yaitu Undang-Undang ITE, menegaskan bahwa kegiatan melalui media sistem elektronik, yang juga dikenal sebagai ruang siber (cyber space), dapat dianggap sebagai tindakan atau perbuatan hukum yang nyata meskipun bersifat virtual.

Hanya saja, ketika terkait dengan kejahatan yang melibatkan teknologi informasi, pembuktian menjadi sulit dilakukan. KUHP sebelumnya tidak memperluas pengertian terkait kegiatan yang dilakukan di ruang siber (cyber space), dan hal ini menyebabkan kendala dalam proses peradilan pelaku kejahatan tersebut. Ketiadaan undang-undang yang mengatasi isu-isu teknologi informasi dapat menyebabkan pelaku kejahatan tidak dapat dihukum, dan jika hal ini tidak segera diatasi, dapat menimbulkan ketidakpuasan di masyarakat. Oleh karena itu, penyelesaian cepat terhadap permasalahan ini menjadi penting agar keadilan dapat ditegakkan dan keamanan di ruang siber dapat dijaga, mencegah potensi keresahan di tengah masyarakat.

Menurut penulis ada dua kendala utama pembuktian dalam kejahatan carding. Kendala pertama terkait dengan mendapatkan alat alat bukti yang sah mengalami kesulitan dalam mengakses alat bukti keterangan saksi karena tindakan kejahatan tersebut terjadi di ranah maya. Oleh karena itu, sebagian besar alat bukti dalam kasus semacam ini cenderung bergantung pada keterangan ahli untuk menyajikan bukti yang relevan dan memahami aspek-aspek teknis terkait dengan kejahatan carding tersebut, sementara kendala kedua berkaitan dengan keterbatasan sumber daya manusia dalam proses pembuktian. Dalam upaya penindakan untuk memberantas cybercrime, terdapat kekurangan sumber daya manusia di kalangan aparat penegak hukum. Hal ini disebabkan oleh kebutuhan akan keahlian khusus di bidang komputer dalam rangka efektif menanggulangi tindak pidana ini.

Selain itu penulis memiliki argument bahwa untuk kasus kejahatan carding atau mencuri data kartu kredit komputer orang lain secara ilegal, dalam penyidikannya dihadapkan problematika yang rumit, terutama dalam hal pembuktian. Banyak saksi maupun tersangka yang berada di luar yurisdiksi hukum Indonesia, sehingga untuk melakukan pemeriksaan maupun penindakan amatlah sulit, belum lagi kendala masalah bukti-bukti yang amat rumit terkait dengan teknologi informasi dan kode-kode digital yang membutuhkan sumber daya manusia serta peralatan komputer forensik yang baik. Dalam modus carding data yang dicuri tersebut sama sekali tidak berubah. Hal tersebut baru diketahui biasanya setelah selang waktu yang cukup lama karena orang yang mempunyai uang yang telah dicuri mengetahui setelah merasa uangnya berkurang dan tidak merasa mengambilnya, hal ini bisa diketahui dalam hal yang lama apabila korban juga melihat uangnya dikemudian hari. Hal ini disebabkan karena pada saat kejahatan berlangsung atau dilakukan tidak ada satupun saksi yang melihat. selain itu, untuk kasus carding, permasalahan yang ada adalah saksi korban kebanyakan berada di luar negeri sehingga sangat menyulitkan dalam melakukan pelaporan dan pemeriksaan untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban.

Upaya Perbankan dalam Pengamanan Data Kartu Kredit Nasabah

Dari banyaknya kasus kejahatan carding membuat banyak pemegang kartu yang merasa tidak aman meninggalkan uangnya pada bank dan dalam hal ini menyebabkan ketidakpercayaan pemegang kartu kredit terhadap bank. Karena itu, bank wajib merahasiakan dan melindungi nasabahnya dengan cara melakukan pengamanan terhadap data nasabah kartu kredit. Hal ini juga dilakukan untuk mengembalikan kepercayaan para nasabah kepada bank.

Dalam upayanya Pasal 21 Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 11 /Pojk.03/2022 Tentang Penyelenggaraan Teknologi Informasi (POJK PTI) Oleh Bank Umum menjelaskan mengenai ketahan dan keamanan siber bank Untuk melaksanakan Pasal 21 POJK No. 11 Tahun 2022 PTI upaya bank dalam upaya menjaga ketahanan siber harus melakukan beberapa proses yaitu, identifikasi aset, ancaman, dan kerentanan; perlindungan asset; deteksi

insiden siber; dan penanggulangan dan pemulihan insiden siber. Hal tersebut dijelaskan lebih lanjut dalam Surat Edaran Otoritas Jasa Keuangan Republik Indonesia Nomor 29 /Seojk.03/2022 Tentang Ketahanan Dan Keamanan Siber Bagi Bank Umum.

Dalam proses identifikasi aset, ancaman, dan kerentanan bank di haruskan untuk melakukan manajemen aset dengan cara melakukan inventarisasi dan penilaian aset Teknologi Informasi, seperti perangkat keras, perangkat lunak, jaringan, dan infrastruktur. Penting juga untuk mencatat konfigurasi secara efektif guna memahami dan mengelola aset-aset tersebut. Selain itu bank juga perlu mengidentifikasi kerentanan dan memantau perkembangan siber terkini untuk dapat mengenali ancaman siber yang mungkin muncul. Hal ini melibatkan pemantauan secara aktif terhadap potensi risiko keamanan yang dapat mempengaruhi aset-aset Teknologi Informasi. Bank juga harus melakukan pengujian keamanan siber secara berkala guna menilai tingkat keamanan sistem dan infrastruktur. Pengujian ini membantu bank dalam mengidentifikasi dan mengatasi potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak berwenang. Berikut langkah-langkah yang dilakukan oleh bank terkait dengan perlindungan, deteksi dan penanggulangan kejahatan siber; Proses Pelindungan Asset Yang Dilakukan Oleh Bank sebagai berikut ;

1. Menerapkan pengendalian keamanan yang komprehensif sesuai dengan hasil identifikasi aset, ancaman, dan kerentanan yang telah diidentifikasi sebelumnya.
2. Melakukan pemeliharaan dan perbaikan terhadap pengendalian keamanan atas aset TI sesuai dengan kebijakan dan prosedur yang berlaku, untuk memastikan bahwa kontrol keamanan tetap efektif.
3. Menerapkan sistem pengamanan yang dikelola dengan baik sesuai kebijakan dan prosedur yang berlaku, guna memastikan bahwa sistem tersebut dapat memberikan tingkat perlindungan yang optimal.
4. Melakukan peninjauan pengendalian keamanan secara berkala untuk memastikan kecukupan kontrol keamanan yang digunakan, sesuai dengan hasil terkini dari proses identifikasi.
5. Menerapkan manajemen keamanan data dan informasi serta memastikan bahwa data dan informasi dikelola sesuai dengan strategi manajemen risiko organisasi, termasuk perlindungan terhadap kerahasiaan, integritas, dan ketersediaan data dan informasi.
6. Menerapkan manajemen pelindungan terhadap jaringan, perangkat keras, dan perangkat lunak untuk mengurangi risiko terhadap keamanan sistem.
7. Menerapkan manajemen pelindungan terhadap akses dan pengguna untuk mencegah tindakan tidak terotorisasi pada perangkat, infrastruktur jaringan, dan komponen sistem yang dikelola oleh bank.
8. Menerapkan pelindungan yang memadai dalam pelaksanaan kerja sama antara bank dengan pihak penyedia jasa TI, termasuk penggunaan cloud computing.
9. Memastikan penerapan secure coding dalam pengembangan sistem dan aplikasi untuk meminimalisasi kerentanan atas sistem dan aplikasi.
10. Memastikan pelaksanaan patching berjalan dengan baik serta memastikan keandalan dan kemutakhiran seluruh komponen perangkat lunak, jaringan komunikasi, database, dan sistem operasi bank.

langkah-langkah yang dilakukan oleh bank terkait dengan perlindungan, deteksi dan penanggulangan kejahatan siber;Proses Deteksi Insiden Siber Yang Dilakukan Oleh Banksebagai berikut ;

1. Memastikan ketersediaan dokumentasi kinerja dasar atas fungsi kritis bank dan sistem pendukung. Hal ini bertujuan untuk mendeteksi penyimpangan dengan tepat waktu serta menandai aktivitas dan kejadian anomali guna dilakukan tindaklanjut.
2. Melakukan pemantauan atas aktivitas mencurigakan dan mengelola serta menguji proses dan prosedur deteksi. Tujuannya adalah untuk memastikan bahwa aktivitas anomali dapat dideteksi dengan cepat, sehingga bank dapat merespons dengan efektif.
3. Melakukan pemantauan atau deteksi berkelanjutan terhadap kerentanan guna memastikan efektivitas dari upaya pelindungan yang telah diterapkan sebelumnya.
4. Menjamin ketersediaan proses yang memadai untuk mendeteksi insiden siber. Ini

mencakup pembangunan dan pemeliharaan sistem deteksi yang dapat memberikan peringatan dini terhadap potensi ancaman.

5. Melakukan analisis terhadap ancaman dan kerentanan yang terkait dengan suatu insiden siber. Hal ini bertujuan untuk memastikan penanganan insiden secara efektif, mencegah gangguan pada layanan dan/atau operasional bank, dan mengurangi dampak yang mungkin timbul.

langkah-langkah yang dilakukan oleh bank terkait dengan perlindungan, deteksi dan penanggulangan kejahatan siber; Proses Penanggulangan dan Pemulihan Insiden Siber yang dilakukan oleh Bank sebagai berikut ;

1. Menyusun rencana penanggulangan dan pemulihan insiden siber untuk memastikan penanganan dan pemulihan layanan dilakukan secara tepat waktu, sesuai dengan tingkat risiko yang ada, dan dengan dampak minimal.
2. Menetapkan peran, tugas, dan tanggung jawab tim tanggap insiden siber untuk memastikan penanggulangan dan pemulihan insiden siber dilaksanakan dengan minimal dampak terhadap layanan dan operasional bank.
3. Melaksanakan prosedur pemulihan dan upaya untuk mencegah penyebaran dampak dari insiden siber dengan melakukan mitigasi dan tindakan penanggulangan yang sesuai.
4. Melakukan analisis untuk memastikan bahwa langkah-langkah penanggulangan dan pemulihan insiden siber dijalankan dengan tepat dan efektif.
5. Melakukan eskalasi dan pelaporan insiden siber sesuai dengan jalur komunikasi yang telah ditetapkan, untuk memastikan respons yang cepat dan koordinasi yang efisien.
6. Melakukan analisis pasca-insiden sebagai pembelajaran, dengan tujuan memperoleh wawasan yang berharga (lesson learned) dari pengalaman tersebut, guna mendukung perbaikan berkelanjutan dalam penanggulangan dan pemulihan insiden siber di masa mendatang.

D. Kesimpulan

Berdasarkan pembahasan dalam penelitian ini, peneliti menyimpulkan beberapa hasil penelitian sebagai berikut:

1. Faktor-faktor penyebab sulitnya pembuktian dalam kejahatan carding di indonesia yaitu untuk mendapatkan alat bukti yang sah cukup sulit karena kendala masalah bukti-bukti yang amat rumit terkait dengan teknologi informasi dan kode-kode digital yang membutuhkan sumber daya manusia serta peralatan komputer forensik yang baik. Selanjutnya banyak saksi maupun tersangka yang berada di luar yurisdiksi hukum Indonesia, sehingga untuk melakukan pemeriksaan maupun penindakan amatlah sulit, belum lagi permasalahan yang ada adalah saksi korban kebanyakan berada di luar negeri sehingga sangat menyulitkan dalam melakukan pelaporan dan pemeriksaan untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban
2. Upaya penanggulangan kejahatan carding yang dilakukan perbankan dalam pengamanan data nasabah kartu kredit di indonesia dilakukan dengan cara, yaitu sesuai dengan Pasal 40 ayat (1) UU No. 10 Tahun 1998 tentang Perbankan, diatur bahwa bank memiliki kewajiban menjaga kerahasiaan informasi mengenai nasabah penyimpan dan simpanannya. Kewajiban ini mencakup perlindungan terhadap data nasabah dalam posisinya sebagai penyimpan. Dalam upaya bank dalam menjaga ketahanan siber harus melakukan beberapa proses yaitu, identifikasi aset, ancaman, dan kerentanan; perlindungan asset; deteksi insiden siber; dan penanggulangan dan pemulihan insiden siber. Hal tersebut dijelaskan lebih lanjut dalam Surat Edaran Otoritas Jasa Keuangan Republik Indonesia Nomor 29 /Seojk.03/2022 Tentang Ketahanan Dan Keamanan Siber Bagi Bank Umum.

Acknowledge
Puji dan syukur peneliti ucapkan kehadiran Allah SWT, atas segala berkah, rahmat, dan karunia-Nya yang telah memberikan ilmu pengetahuan, pengalaman, kekuatan, kesabaran, dan kesempatan kepada peneliti sehingga mampu menyelesaikan artikel ini. Akan tetapi sesungguhnya peneliti menyadari bahwa tanpa bantuan dan dukungan dari berbagai pihak, maka penyusunan skripsi ini tidak dapat berjalan dengan baik.Hingga selesainya penulisan skripsi ini telah banyak menerima bantuan waktu, tenaga dan pikiran dari banyak pihak.

Daftar Pustaka

[1] Kotler P. *Manajemen Pemasaran [Internet]*. Jakarta: Indeks; 2005. Available from: Leonard Tiopan Panjaitan, Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang- Undang Informasi dan Transaksi Elektronik no.11 Tahun 2008, Artikel Jurnal Telekomunikasi dan Komputer Vol 3 No 1, 2017.

[2] Salsabila Aufadhia Ilanoputri, Prinsip Kerahasiaan Bank Dan Self Assessment System Dikaitkan Dengan Undang-Undang Akses Informasi Keuangan Sebagai Upaya Penegakan Kepatuhan Pajak, Jurnal Program Magister Hukum Fakultas Hukum Universitas Indonesia Vol. 2, No.1.

[3] Yudistira, M., & Ramadani, R. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo. Unes Law Review, Volume 5(4)

[4] Arnold Bagas Kurniawan,"Perlindungan Hukum Kepada Pengguna Elektronik Banking Atas Kejahatan Carding Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik", Supremasi Jurnal Hukum, Vol. 5, No. 1, 2022.

[5] https://www.akki.or.id/index.php/credit-card-growth

[6] Antonius Maria Laot Kian, "Tindak Pidana Credit/Debit Card Fraud dan Penerapan Sanksi Pidananya dalam Hukum Pidana Indonesia," Hasanuddin Law Review, 1 2015.

[7] Baldwin Orvalla, & Eka Juarsa. (2023). Pertanggungjawaban Pidana Anggota Densus 88 dalam Tindak Pidana Pembunuhan Berencana Dihubungkan dengan Pasal 340 KUHP. *Jurnal Riset Ilmu Hukum*, 107–110. https://doi.org/10.29313/jrih.v3i2.2873

[8] Fauzia, S., 1∗, M., & Mahmud, A. (2023). Penegakan Hukum Tindak Pidana Penipuan melalui Aplikasi Pencarian Jodoh Tinder dan Upaya Pencegahannya (Vol. 01). https://journal.sbpublisher.com/index.php/LOL

[9] Romero, A. N., Sri Ratna Suminar, & Zakiran, A. H. (2023). Pemenuhan Hak Pasien BPJS dalam Mendapatkan Pelayanan Antidiskriminasi Dihubungkan dengan UU Rumah Sakit. *Jurnal Riset Ilmu Hukum*, 31–36. https://doi.org/10.29313/jrih.v3i1.2121