BAB II

KEJAHATAN TRANSNASIONAL CARDING CRIME DAN NCB INTERPOL INDONESIA

2.1 Definisi dan Karakteristik *Carding Crime*

Pada dasarnya *Carding Crime* merupakan kejahatan yang berada pada ranah *Cyber Crime* dikarenakan hal ini masuk dalam definisi yang telah dibuat oleh Majid Yar, dan Kevin F Steinmetz yaitu merujuk pada tindak pidana yang dilakukan melalui pemanfaatan jaringan komputer atau menargetkan sistem komputer dan data (Marita, 2019) (Yar & Steinmetz, 2019). *Carding Crime* memanfaatkan pencurian, penyalahgunaan, dan perdagangan data kartu kredit atau debit lewat jaringan digital. Sasaran dari metode *carding* ini juga tidak hanya menyasar lewat kartu kredit namun hal ini juga berlaku dengan debit, dan mobile banking maupun yang lain.

Kejahatan ini telah berevolusi sehingga tidak memerlukan lagi kartu fisik untuk melancarakan kejahatannya atau yang sering disebut sebagai *Card-Not-Present Fraud*. Sehingga pencurian kartu kredit ini memiliki karakteristik *borderless* dikarenakan bisa mentargetkan korban dimanapun tempatnya dan tidak mengenal batas negara. Pola lintas batas ini membuatnya di kategorikan menjadi kejahatan *Transnasional* sebagaimana diuraikan oleh UNODC pada tahun 2013 bahwa *Cybercrime* disebut sebagai kejahatan transnasional apabila pelaku, korban, sarana, atau akibatnya melebihi dari satu negara.

2.1.1 Card-Not-Present Fraud

Carding telah berevolusi dari cara cara konvensional yang membutuhkan kartu fisik menjadi sebuah kejahatan dengan metode-metode tertentu seperti *Card Not Present* yang dimana menurut Europol, kejahatan tetap dapat terjadi meskipun tidak secara langsung menargetkan kartu kredit/debit nya. Pelaku bisa melakukannya tanpa adanya kartu fisik yang hadir sehingga menargetkan data pribadi dan juga informasi yang diperlukan untuk menerobos sistem keamanan seperti, *e-commerce, subscription platform,* dan layanan digital. Hal ini sekarang marak terjadi dengan menggunakan metode-metode serangan digital dan lebih efektif memakan korban karena bisa menargetkan korban lebih banyak daripada cara-cara konvensional.

Kejahatan *carding* tidak lagi berdiri sendiri namun menjadi sebuah fase monetisasi akhir dari sebuah rangkaian aktivitas data *harvesting. D*ata *harvesting* ini dapat melalui banyak sekali metode seperti *phising*, *skimming*, *malware injection* maupun data breach yang targetnya adalah data pribadi dari korban dalam upaya menemukan *payment credentials* yang dapat memberikan akses menuju ke instrumen keuangan korban baik *mobile banking*, atau kartu digital. *Carding* telah menjadi kejahatan terorganisir yang menerapkan sistem *interconnectedness of cybercrime* dimana sebuah kejahatan siber saling terhubung antara satu dengan yang lainnya (Huang, 2024). Terdapat spesialisasi peran dalam ekosistem kejahatan, aktor yang pertama

melakukan inflitrasi dengan modus-modus operandi untuk mendapatkan data pribadi dari korban, lalu kemudian aktor selanjutnya menggunakan data tersebut untuk melakukan transaksi ilegal ataupun dijual di pasar gelap seperti *atau darkweb (carding forums)* hal ini dapat disebut sebagai *Cybercrime-as-a-Service* (CaaS) (EUROPOL, 2025).

2.1.2 Modus Operandi *Carding Crime*

Dalam melancarkan serangannya, pelaku kejahatan *carding* atau biasa di sebut *carder* biasanya tidak hanya menggunakan satu metode kejahatan, pelaku sering kali melakukan beberapa metode sekaligus sehingga meningkatkan probabilitas dalam melakukan pencurian kartu kredit dan data pribadi seseorang yang menghasilkan kerugian material. Serangan dan metode ini dilakukan sebagai tahap awal untuk terjadinya *carding* yang terkoneksi satu sama lain dan secara tidak langsung serangan-serangan ini merupakan bentuk dari *carding* itu sendiri. Terdapat berbagai metode dalam melaksanakan *carding,* antara lain yang paling umum digunakan adalah sebagai berikut :

2.1.2.1 Phishing

Phishing merupakan sebuah modus oprerandi yang sering kali dipakai oleh para pelaku *Carding* yang dimana *Phishing* merupakan sebuah metode rekayasa sosial, pelaku membuat sebuah situs palsu, email palsu, maupun pesan tiruan atau notifikasi palsu berbentuk institusi resmi, yang paling umum adalah bank, *e-commerce,* payment gateway, hadiah undian, dan masih banyak

yang lainnya (Anti Phising Working Group, 2025). Jika korban mengakses situs palsu tersebut maka pelaku akan mendapatkan jenis data pribadinya. Biasanya dalam kasus *Carding* pelaku memancing korban sehingga dapat mengambil data nomor kartu (PAN), tanggal kadaluwarsa, CVV/CVC, OTP maupun 3D secure yang lain.

2.1.2.2 Malware Injection / Magecart

Metode *Malware Injection* merupakan metode dimana seorang pelaku kejahatan melakukan penanaman *malware* yang dirancang untuk mendapatkan data diri korban. Pertama-tama pelaku melakukan metode pemalsuan link download, email attachment palsu, atau *malversting* (iklan palsu) sehingga dapat disusupkan *malware.* Banyak korban yang tidak dapat membedakan dikarenakan bentuknya yang mirip dan dibuat sedemikian rupa oleh pelaku sehingga banyak korban yang tertipu. Malware dalam sistem ini bekerja sebagai: *Keylogger* yang merekam penekan tombol saat korban mengetik data kartu*, Spyware* yang menangkap *screenshot* saat korban melakukan aktifitas krusial seperti pembayaran, *Formjacking* menyisipkan script pada website-website jual beli atau e-commerce untuk mencuri data saat korban sedang melakukan aktifitas transaksional.

Dalam kasus tertentu *malware injection* biasa disebut *magecart attack* ini merupakan bentuk digital skimming yang kerap sekali terjadi dalam kasus *carding.* Pelaku melakukan penyuntikan

kode *JavaScript* berbahaya yang menyasar langsung platform *e-commerce* untuk mencuri datanya secara *real-time.*

2.1.2.3 Skimming

Skimming merupakan metode dimana pelaku kejahatan melakukan penyalinan data kartu pembayaran melalui perangkat atau teknik tertentu ketika kartu digunakan pada mesin yang sah seperti mesin ATM, EDC, atau terminal pemnayaran lain (Skimming Prevention Task Force, 2014). Metode ini sangat umum digunakan karena merupakan salah satu metode paling konvensional yang dalam kejahatan *carding* sebelum berevolusi menjadi serangan-serangan *Card Not Present.* Skimming mengambil data strip magnetik atau chip sehingga dapat melakukan cloning terhadap kartu debit maupun kredit. Saat ini metode skimming ini sering digunakan untuk jual beli di forum darknet atau forum ilegal.

2.1.2.4 Online Scam

Online scam didefinisikan sebagai skema penipuan yang memanfaatkan teknologi informasi dan komunikasi untuk memanipulasi korban agar memberikan aset finansial, data pribadi, atau kredensial sensitif lainnya. Menurut *Global Anti Scam Alliance* (GASA), *online scam* telah berevolusi menjadi ancaman transnasional yang sistematis dimana para aktor kejahatan menggunakan teknik rekayasa *sosial engineering* untuk menciptakan narasi dengan tujuan mengelabui target melalui berbagai platform digital (Global Anti Scam Alliance, 2025).

Dalam langkap kejahatan siber finansial, *online scam* berperan sebagai metode infiltrasi awal yang krusial. Praktik ini seringkali bermanifestasi dalam bentuk situs belanja palsu atau penipuan investasi yang bertujuan untuk melakukan pencurian data. Berbagai bentuk *scam* telah berubah seiring berjalannya waktu sehingga ini bukan hanya merupakan penipuan satu arah, namun sebuah instrumen strategis dalam rantai pasok kejahatan siber.

2.1.2.5 Carding as a Service (CaaS)

Carding-as-a-Service (CaaS) merupakan sebuah model bisnis kriminal di mana seluruh komponen kejahatan *carding* tersedia sebagai layanan modular yang dapat dibeli secara terpisah: data kartu curian, alat validasi kartu, *proxy* anonim, hingga layanan *money mule* untuk pencucian hasil kejahatan. Pasar gelap seperti BidenCash (aktif sejak 2022), BriansClub (aktif sejak 2015), dan B1ack's Stash (2024) secara agresif mempromosikan diri dengan membagikan jutaan data kartu curian secara gratis sebagai strategi pemasaran untuk menarik pelanggan baru (Blia et al., 2026). Pada April 2024, B1ack's Stash membagikan satu juta data kartu curian secara gratis dalam satu gelombang tunggal sebagai perayaan peluncuran toko gelapnya, hal ini merupakan bukti bahwa dalam ekosistem kejahatan memiliki kematangan dalam mempromosikan toko gelap tersebut (Catoto Santos, 2026).

2.2 Sejarah INTERPOL

Interpol merupakan organisasi kepolisian internasional yang bertujuan untuk memfasilitasi kerja sama penegakan hukum antarnegara dalam menangani kejahatan lintas batas. Secara historis sendiri Interpol berawal dari pembentukan *Internasional Criminal Police Commision* (ICPC) pada tahun 1923 di Vienna, Austria. Pembentukan ini ditujukan untuk meningkatkan koordinasi kepolisian antarnegara dalam menghadapi gelombang kejahatan internasional pada awal abad ke-20. Kemudian setelah perang Dunia ke 2, organisasi ini di reorganisasi pada tahun 1956 secara resmi mengadopsi nama *Internasional Criminal Police Organization - Interpol* hingga saat ini (Deflem, 2002). Sejak saat itu, Interpol telah berkembang menjadi jaringan kerja sama kepolisian terbesar di dunia dengan lebih dari 190 negara anggota. Markas besar organisasi ini saat ini berada di Lyon, France yang berfungsi sebagai pusat koordinasi operasional serta membantu pengembangan sistem pertukaran informasi kriminal seperti data pelaku kejahatan, metode operasi kriminal, serta jaringan kejahatan transnasional lain. Dalam praktiknya Interpol berperan menjadi mekanisme koordinasi bagi negara dalam menghadapi ancaman-ancaman keamanan non-tradisional seperti kejahatan transnasional seperti perdagangan manusia, narkotika, terorisme, dan kejahatan siber.

Interpol sendiri menjadi salah satu institusi besar yang membantu banyaknya negara dalam melawan kejahatan salah satunya kejahatan *cyber*.

Melalui *Cybercrime Directorate*, Interpol mendukung negara-negara anggota dalam melakukan pertukaran intelijen kriminal, pelacakan pelaku kejahatan siber, pengembangan kapasitas penyidik, serta koordinasi operasi lintas negara. INTERPOL juga mengembangkan berbagai instrumen pendukung seperti jaringan komunikasi aman I-24/7 yang memungkinkan aparat penegak hukum di negara anggota untuk mengakses dan bertukar informasi secara real-time mengenai individu, kelompok, maupun jaringan kejahatan yang sedang menjadi target penyelidikan. Melalui mekanisme tersebut, Interpol membantu mengurangi hambatan yurisdiksi yang sering kali menjadi kendala utama dalam penanganan kejahatan siber transnasional. Oleh karena itu, keberadaan Interpol menjadi penting sebagai wadah koordinasi yang memungkinkan terjadinya pertukaran informasi, pelaksanaan investigasi bersama, peningkatan kapasitas aparat penegak hukum, serta pengembangan strategi kolektif dalam menghadapi ancaman kejahatan siber transnasional, termasuk carding crime.

2.3 NCB INTERPOL Indonesia

2.3.1 *National Central Bureau*

Dalam menjalankan fungsi koordinasi tersebut, negara-negara anggota Interpol diwajibkan untuk membentuk *National Central Bureau* (NCB) sebagai penghubung antara kepolisian nasional dengan jaringan interpol global. NCB berfungsi menjadi pusat komunikasi utama yang mengoordinasikan pertukaran informasi kriminal, permintaan bantuan

dalam investigasi dan koordinasi operasi kepolisian lintas negara. Melalui jaringan ini komunikasi global Interpol yang dikenal sebagai I-24/7 membuat NCB dapat mengakses berbagai database internasional mengenai individu yang dicari, dokumen yang hilang atau dicuri serta informasi kriminal lainnya.

2.3.2 NCB Interpol Indonesia sebagai Lembaga Negara

Indonesia sendiri merupakan negara yang tergabung dalam satuan kerja sama internasional Interpol sehingga kerja sama tersebut ter manifestasikan dalam sebuah lembaga yang dinamakan NCB Interpol Indonesia. Lembaga ini berada dibawah Divisi Hubungan Internasional Polri dan menjalankan tugas terkait hubungan internasional antara Polri dan lembaga kepolisian di negara-negara lain dan organisasi (Sekertariat Jenderal) (Rakhmadani & Program, 2016).

2.3.3 Tugas dan Fungsi NCB Interpol Indonesia

Sebagai bagian dari organisasi Interpol maka NCB Interpol Indonesia memiliki kewenangan dalam menangani bentuk-bentuk kejahatan siber transnasional (*transnasional cybercrime)* yang berada dalam wilayah Indonesia dikarenakan Interpol merupakan instrumen dalam kerja sama penegakan hukum yang di bahas pada *The Regime Complex for Managing Global Cyber Activities* (Nye, 2014). Interpol merupakan satu-satunya bentuk kerja sama kepolisian yang bersifat internasional dan memiliki jaringan dengan 190 kepolisian nasional dari negara-negara lain di dunia. Kemudian sebagai bagian dalam organisasi

Polri maka NCB Interpol Indonesia memiliki kewenangan berdasarkan Undang-Undang Nomor 2 tahun 2002 mengenai Tugas Pokok Kepolisian Negara Republik Indonesia, terkhusus pada Pasal 13 dan 15(e) yang disebutkan dimana Polri merupakan sebuah lembaga yang berwenang untuk mengayomi dan melindungi masyarakat dengan cara melakukan penegakan hukum dan berwenang untuk melakukan kerja sama dengan kepolisian negara lain dalam menyidik dan memberantas kejahatan internasional dan juga mewakili pemerintah Republik Indonesia dalam organisasi kepolisian internasional.