Cyber Crime Dan *Fraud* Kartu Kredit DanKartu Debit: Perspektif Akuntansi

Apriwandi[1*], Herycson[2]
[1,2]Universitas Widyatama
Email: apri.wandi@widyatama.ac.id [1*]

Abstrak

Berkembangnya teknologi informasi dan penggunaannya di dalam kehidupan sosial dan ekonomi termasuk pemanfaatannya dalam bertransaksi keseharian termasuk enggunaan kartu kredit dan kartu debit yang sudah umum dilakukan oleh pelaku bisnis memiliki celah untuk terjadinya tindak kejahatan siber. Dalam makalah ini penulis ingin menjabarkan bagaimana karakteristik tindak kejahatan siber (cyber crime) dan penipuan (fraud) kartu kredit dan kartu debit dan upaya pencegahannya dalam perspektif akuntansi. Cyber crime dan fraud terjadi dengan melakukan pemalsuan kartu kredit/debit dan pemalsuan identitas pemegang kartu dan dengan pengembangan sisitem informasi akuntasi juga mengoptimalkan peran akunting dalam hal ini akuntan melalui kontrol internal yang tepat untuk mencegah terjadinya tindak pidana siber (cybercrime) dan penipuan (fraud).

Keyword*: Cyber crime, Kecurangan, Perspektif akuntansi*

PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan penyebarannya secara praktis di semua bidang kehidupan sosial-ekonomi di negara manapun telah menjadi tren utama perkembangan umat manusia khususnya pada revolusi digital saat ini atau disebut dengan Revolusi Industri 4.0. Salah satu dampak perkembangan tersebut ditunjukkan dengan adanya transformasi digital pada proses akuntansi terkait dengan pengumpulan, penyimpanan, pengolahan dan penyampaian informasi. Keuntungan digitalisasi tidak dapat disangkal berpengaruh besar pada sektor bisnis yaitu peningkatan kecepatan dan transparansi proses bisnis, pertumbuhan produktivitas tenaga kerja, pengurangan biaya bekerja, peralihan dari dokumen kertas ke dokumen elektronik, pengolahan data dalam volume besar, sinkronisasi arus informasi, percepatan pengambilan keputusan manajerial dan lain-lain (Fullerton & Durtschi, 2011; Petraşcu & Tieanu, 2014; Vaswani, 1997). Terlepas dari berbagai keuntungannya, teknologi baru juga memiliki celah untuk digunakan melakukan tindak kejahatan, mengobarkan kebencian, memalsukan informasi atau hoax, dan pencurian data pribadi.

Menurut data laporan *World Economic Forum*, serangan siber termasuk dalam lima bahaya utama yang mengancam umat manusia, seperti bencana alam dan perubahan iklim. Kejahatan dunia maya, yang tujuan utamanya adalah perampasan properti (termasuk perampokan aset dari rekening bank) dari pemiliknya, memiliki bahaya khusus. Laporan TechRadar

mengungkapkan laporan tahunan FBI mengenai *Internet Crime Complaint* Center (I3C) atau Pusat Keluhan Kejahatan di Internet sepanjang 2021. Hasilnya, menurut FBI, para korban menderita kerugian sebanyak USD 6,9 miliar atau setara Rp 100,3 triliun akibat berbagai penipuan online yang terjadi.

Peningkatan lalu lintas internet telah menarik pelaku-pelaku kriminal siber dan berakibat pada banyaknya kasus serangan siber di Indonesia. Badan Siber dan Sandi Negara (BSSN) mencatat serangan siber tahun 2020 angka mencapai angka 495,3 juta atau meningkat 41 persen dari tahun sebelumnya 2019 yang sebesar 290,3 juta. Sama halnya dengan Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim), yang melihat adanya peningkatan laporan kejahatan siber. Dimana pada tahun 2019 terdapat 4.586 laporan polisi diajukan melalui Patrolisiber (laman Wet Bareskrim untuk melaporkan kejahatan siber) meningkat dari tahun sebelumnya 4.360 laporan pada 2018 (Dornadula & Geetha, 2019; Gunadi, 2001).

Dari berbagai jenis *cyber crime* yang terjadi di Indonesia, salah satu tindakan kejahatan siber yang terjadi yaitu *carding.* Makna dari c*arding* dalam bahasa formal atau bahasa hukum, dapat dikatakan sebagai salah satu bentuk tindak kejahatan siber yang berkaitan dengan alat pembayaranperbankkan yaitu kartu kredit/kartu debit (*credit/debit card fraud* (Aseri & Gera, 2014; Hille et al., 2016). Pelaku dari tindakan kejahatantersebut seringkali sebut dengan *carder*. Salah satu contoh *carding* yaitu penipuan pada penggunaan kartu kredit yang mana(Dornadula & Geetha, 2019) pelaku mengetahui nomor kartu kredit korbannya yang masih berlaku untuk digunakan, maka pelaku dapat membeli barang secara *on-line* yang tagihannya bisa dialamatkan pada pemilik asli kartu kredit tersebut.

Tindak kejahatan *cyber* khususnya *credit/debit card fraud* tidak hanya merugikan individu, namun juga dapat berdampak pada perusahaan. Untuk mempermudah transaksi perusahaan seringkali menerbitkan kartu kredit atau kartu tagihan yang dipegang oleh karyawan tertentu, tetapi ada risiko dengan keputusan itu, seperti karyawan yang menggunakan kartu tersebut untuk pengeluaran pribadi. Resiko lain yang dapat dialami perusahaan adalah perusahaan berisiko mengalami pembobolan *credit/debit card* yang disebabkan oleh penggunaan kartu kredit / debit milik perusahaan oleh pihak yang tidak bertanggug jawab.

Dengan adanya risiko tersebut, dari perspektif akuntansi maka diperlukan sistem pengamanan yang dapat diterapkan salah satunya yaitu melalui pengawasan internal. Akunting memiliki peranan penting dalam pelaksanaan pencegahan *credit/debit card fraud* dalam perusahaan. Menurut *PricewaterhouseCoopers* (PwC) secara internal 29% dari penipuan yang dilakukan

terhadap organisasi dilakukan oleh karyawan. Secara eksternal perusahaan tidak selalu memiliki sumber daya (waktu, tenaga, uang, dan keahlian) untuk melakukan pencegahan kejahatan siber. Oleh karena itu dalam makalah ini, penulis akan lebih dalam membahas mengenai *cyber crime* khususnya pada *credit/debit card fraud* dalam perspekif akuntansi.

METODE

Penelitian mengenai cybercrime dan fraud bagi pengguna kartu debit dan kredit dalam perspektif akuntansi menggunakan metode kualitatif dengan studi literatur dan kasus sebagai desain penelitiannya. Pada penelitian ini peneliti menerapkan paradigma konstruktivis, sehingga peneliti memandang keadaan sosial sebagai analisis sistematis terhadap respon sosial atas suatu kecurangan dalam kartu debit/kredit pebankan melalui pengamatan langsung dan terperinci terhadap pelaku sosial.

Penelitian ini memfokuskan kajian pada perspektif akuntansi mengenai pola-pola pengendalian kejahatan dunia maya dan kecurangan perbankan. Penjahat dunia maya menggunakan teknologi komputer untuk mengakses atau mengeksploitasi data pribadi atau rahasia dagang bisnis, biasanya untuk tujuan jahat.

Paradigma Konstruktivis atau Konstrutivisme Sosial (Ghozali, 2011; Jogiyanto Hartono, 2015) dijelaskan bahwa peneliti berusaha memahami secara langsung dunia tempat mereka hidup dan bekerja, serta melakukan penelitian atas permasalahan yang dihadapi dan dirasakan. Pengembangan makna subjektif untuk menjelaskan berdasarkan pengalaman peneliti langsung yang mengarah pada objek tertentu.

HASIL DAN PEMBAHASAN.

Karakteristik Tindak Kejahatan *Credit /Debit Card Fraud*

Kejahatan dunia maya adalah kejahatan di mana komputer menjadi target, atau alat, untuk melakukan pelanggaran, melalui spamming atau peretasan informasi. Penjahat dunia maya menggunakan teknologi komputer untuk mengakses atau mengeksploitasi data pribadi atau rahasia dagang bisnis, biasanya untuk tujuan jahat.

Individu bukan satu-satunya target penipuan kartu kredit. Dengan tuntutan sehari-hari dalam menjalankan perusahaan, pemilik bisnis dapat dengan mudah lengah dan membiarkan keuangan mereka rentan terhadap aktivitas kriminal yang mengarah pada implikasi keuangan yang serius. Dalam tindak kejahatan *credit /debit card fraud* pelaku dapat melakukan aktivitas penipuan online dengan mendapatkan rincian penting seperti nomor rekening dan nama pemegang. Dan mereka dapat melakukannya melalui surat atau melalui telepon dimana kartu kredit fisik tidak diperlukan untuk melakukan penipuan. Selain itu beberapa pelaku juga dapat menggunakan kartu debit yang hilang

atau dicuri untuk melakukan transaksi yang tidak sah.

Kartu kredit umumnya mengacu pada kartu yang diberikan kepada pelanggan (pemegang kartu), biasanya memungkinkan mereka untuk membeli barang dan jasa dalam batas kredit tertentu. Kartu kredit memberikan keuntungan waktu kepada pemegang kartu, yaitu memberikan waktu bagi pelanggan untuk membayar kemudian dalam waktu yang ditentukan, dengan menerpkan siklus penagihan berikutnya.

Credit card fraud atau penipuan kartu kredit merupakan sasaran empuk bagi pelaku cybercrime. Dengan metode tertentu jumlah yang signifikan dapat ditarik tanpa sepengetahuan pemilik, dalam waktu singkat. Penipu selalu berusaha membuat setiap transaksi penipuan terlihatsah, yang membuat deteksi penipuan sangat sulit dilacak dan sulit untuk dideteksi (Adepoju, O., Wosowei & Jaiman, 2019). Sasaran dari tindakan *credit card fraud* tidak hanya perorangan namun juga perusahaan. Sangat penting bahwasetiap bisnis tetap waspada saat mengelola dan memantau akun kredit mereka.

Credit card fraud ketika seseorang menggunakan kartu kredit orang lain untuk alasan (kepentingan, pen) pribadi sedangkan pemilik kartu dan penerbit kartu tidak menyadari bahwa kartu miliknya sedang digunakan (Chaudhary, 2012; Dornadula & Geetha, 2019; Said Noor Prasetyo, 2016). Selanjutnya, seseorang tersebut menggunakan kartu tanpa ada hubungannya dengan pemegang kartu atau penerbit, dan tidak memiliki niat baik untuk menghubungi pemilik kartu atau membuat pembayaran atas pembelian yang dilakukannya (Arens et al. 2015; Said Noor Prasetyo, 2016). Berdasarkan pada dua pengertian tersebut dapat penulis ambil pengertian bahwa *credit card fraud* adalah tindakan seseorang menggunakan kartu kredit milik orang lain secara melawan hak dengan tujuan untuk mendapatkan sesuatu yang berharga baik untuk menguntungkan dirinya sendiri maupun orang lain dengan maksud untuk menipu.

Merujuk kepada pengertian tersebut, untuk dapat melakukan tindak pidana *credit card fraud*, pelaku harus mendapatkan (secara melawan hukum) kartu kredit milik orang lain terlebih dahulu. Kartu kredit yang dimaksud baik kartu kredit dalam bentuk fisik, maupun data elektronik yang berisi informasi identitas pribadi tentang kepemilikan kartu kredit yang terekam di dalam kartu seperti nama penerbit kartu, nama pemegang kartu, nomer kartu, masa berlaku kartu, maupun nomor verifikasi kartu atau CVV (*Card Verification Value*). Perbuatan penguasaan data identitas pribadi seseorang secara melawan hukum tersebut disebut *identity theft*.

Identity Theft terjadi ketika seseorang memperoleh atau mendapatkan, mengirim, memiliki, atau menggunakan informasi pribadi dari seseorang atau suatu badang hukum dengan cara yang tidak sah, dengan

maksud untuk melakukan, atau sehubungan dengan, penipuan atau kejahatan lainnya.[7] Kejahatan ini jarang dilakukan dengan menjadikan informasi identitas pribadi sebagai target tujuannya. Sebaliknya, kejahatan ini hampir selalu dijadikan sebagai sarana untuk memudahkan kejahatan lain, biasanya kejahatan dalam bidang keuangan dengan memperkaya diri pelaku dengan mengorbankan individu, bisnis, lembaga keuangan, maupun lembaga pemerintah (Adepoju, O., Wosowei & Jaiman, 2019; Dornadula & Geetha, 2019). *Identity theft* ini merupakan perbuatan pendahuluan sebagai sarana untuk melakukan suatu tindak pidana.

Tindak pidana *credit card fraud* ini, terdapat dua tahap besar. Tahap pertama, sebelum dapat melakukan tindak pidana *credit card fraud*, pelaku harus mendapatkan kartu kredit (milik orang lain) atau informasi elektronik berkenaan dengan kartu kredit tersebut terlebih dahulu, seperti *ID Number, expiry date*, *CVV Number*, dsb. Terdapat beberapa teknik/ cara untuk mendapatkan kartu kredit ataupun informasi di dalamnya tersebut misalnya *skimming*, *phishing*, *hacking*, *social engeenering*, dll. Teknik atau metode-metode dalam tahap ini disebut sebagai *identity theft*. Tahap kedua adalah penggunaan data informasi pribadi dari kartu kredit untuk melakukan transaksi tanpa ijin dari pemegang sah kartu kredit (Deloitte, 2013).

Berdasarkan pada penjabaran di atas, dapat dipahami karakter tindak pidana *credit card fraud* bahwa tindak pidana *credit card fraud*, selalu terdiri dari, minimal, dua tindak pidana, yaitu pertama adalah *identity theft*, dan kedua adalah tindak pidana *credit card fraud* itu sendiri. Pelaku menggunakan kartu kredit milik orang lain yang dikuasainya untuk mendapatkan keuntungan secara finansial baik untuk dirinya sendiri maupun orang lain secara melawan hukum. Karakteristik yang dimiliki oleh *credit card fraud* tersebut, dalam ajaran hukum pidana, dikualifikasikan sebagai *concursus*.

Menurut Chaundhary (2012) transaksi berbasis kartu kredit dapat diklasifikasikan menjadi dua jenis. Pertama, transaksi menggunakan kartu kredit dalam bentuk fisik, dan kedua transaksi kartu jarak Jauh. Pada transaksi menggunakan kartu kredit dalam bentuk fisik, pemegang kartu memberikan kartunya secara fisik ke pedagang (*merchant*) untuk melakukan pembayaran. *Credit card fraud* dengan menggunakan metode ini, pelaku harus memiliki kartu kredit dalam bentuk fisik.

Kedua, transaksi kartu jarak Jauh (biasa disebut transaksi *on-line*), pada transaksi jenis ini, hanya membutuhkan beberapa informasi penting tentang kartu, seperti nama pemegang kartu kredit, nomor kartu kredit, Tanggal Kadaluarsa, kode pengaman, nomor verifikasi kartu kredit (CVV) untuk melakukan pembayaran. Untuk melakukan penipuan dalam jenis transaksi ini, pelaku perlu mengetahui rincian informasi penting tentang kartu. Rincian data

itulah yang diberikan kepada pedagang (*merchant*) sebagai alat pembayaran. Dengan informasi itulah pedagang akan membebankan beban pembayaran kepada *account* (rekening) kartu kredit milik pemegang yang sah.

Berdasarkan pada penjabaran di atas, dapat disimpulkan bahwa terdapat beberapa skema *credit card fraud* diantaranya (Chaudhary, 2012; Said Noor Prasetyo, 2016):

a. Pelaku menggunakan kartu kredit (dalam bentuk fisik) asli yang didapatkannya secara melawan hukum untuk berbelanja barang danl atau jasa di toko-toko yang menerima pembayaran dengan kartu kredit, atau menarik uang tunai di mesin ATM yang tentu saja tanpa seijin atau sepengetahuan pemegang sah dari kartu kredit.
b. Pelaku menggunakan kartu kredit (dalam bentuk fisik) palsu yang telah dibuatnya untuk berbelanja barang dan/atau jasa di toko-toko yang menerima pembayaran dengan kartu kredit tanpa seijin atau sepengetahuan pemegang sah dari kartu kredit.
c. Pelaku menggunakan data elektronik terkait kartu kredit seperti nomer kartu kredit, nama pemegang, nama penerbit, tanggal kadaluarsa, kode pengaman, dan nomer varifikasi kartu kredit (CVV: *Card Verification Value*) untuk berbelanja barang danl atau jasa secara *on-line* dengan menyebutkan/ memberikan data kartu kredit tersebut kepada pedagang.

Sedangkan penipuan kartu debit (*debit card fraud*) terjadi ketika seseorang mendapatkan akses ke kartu debit atau detail kartu dan menggunakannya untuk melakukan pembelian atau penarikan yang tidak sah (Setiawan, 2019). Karakteristik utama dalam tindakan siber ini yaitu pelaku biasanya membutuhkan akses langsung bentuk fisik pada kartu debit yang digunakan.

Untuk mengetahui tindak kejahatan ini maka dapat diketahui jika kartu debit yang dimiliki hilang, melihat aktivitas mencurigakan dan tidak dapat dijelaskan di rekening bank, memeriksa tagihan penipuan pada kartu debit. Dan juga dapat melihat adanya laporan mutasi bank yang tidak dilakukan, melihat penarikan di lokasi yang belum dikunjungi, atau tiba-tiba menemukan bahwa terdapat pembayaran terjadwal telah dibatalkan. Cara terbaik untuk tetap waspada adalah dengan memeriksa saldo dan transaksi rekening bank setiap hari menggunakan aplikasi mobile atau onlinebanking.

Namun tidak mengeherankan jika perkembangan teknologi saat ini juga dapat memungkinkanseseorang menggunakan kartu debit tanpa menggunakan kartu fisik. Salah satu metode yang digunakan adalah melalui perangkat *skimming* kartu ATM. Skimming adalah tindakan kejahatan pencurian data pengguna ATM untuk membobol rekening. Untuk melancarkan aksi ini pelaku kejahatan menggunakan alat khusus bernama skammer yang bentuknya mirip dengan mulut slot

kartu ATM (Apriwandi & Supriyono, 2021; Saragih et al., 2019; Setiawan, 2019). Melalui alat tersebut penipu dapat mengetahui detail kartu pemiliknya. Selain metode tersebut juga dapat dilakukan dengan meretas perangkat handphone untuk memperoleh akses ke mobile banking, atau mengarahkan untuk melakukan pembayaran di situs web palsu yang mengumpulkan detail informasi pengguna.

Pencegahan *Cyber Crime* Dan *Fraud* Kartu Kredit Dan Kartu Debit dalam Perspekif Akuntansi

Penipuan selalu ada, namun perkembangan teknologi yang pesat menciptakan peluang baru untuk terjadinya kecurangan. Perlu diketahui kemungkinan dan dampak terjadinya *fraud*, mulai dari faktor manusianya, melalui sistem informasi akuntansi, karena seberapapun berkembangnya teknologi informasi, dampak dari sumber daya manusia tetap ada. Karyawan atau eksekutif yang rentan terhadap penipuan biasanya ambisius, kurangnya perhitungan dan perencanaan yang baik, hidup di atas potensi penghasilan mereka, memiliki masalah sosial dan psikologis serta keuangan (Christine & Apriwandi, 2022; Mitrović & Knežević, 2020).

Kecurangan merupakan kesalahan yang dilakukan secara sengaja dan dapat mengakibatkan terjadinya kerugian terhadap suatu perusahaan. Salah satu faktor yang mempengaruhi terjadinya kecurangan adalah adanya kesempatan yang disebabkan oleh pengendalian internal organisasi yang lemah, kurangnya pengawasan dan adannya penyalahgunaan wewenang pegawai perbankan.

Menurut *PricewaterhouseCoopers* (PwC) dampak kerugian kecurangan atau *fraud* pada perusahaan sangat kompleks. Terdapat kerugian biaya yang dapat diukur seperti kerugian finansial secara langsung, penalti, tanggapan dan ada juga kerugian biaya yang tidak dapat diukur seperti kerusakan merek, kehilangan moral dan kehilangan peluang masa depan. Beberapa jenis kecurangan seperti *eksternal fraud*, pada umumnya menyerang dari luar perusahaan, bersifat transaksional, memungkinkan pemantauan aktif, dan adanya pengelolaan akuntansi dengan benar dapat mengurangi dampak keuangan. ((Deloitte, 2013).

Beberapa upaya yang dilakukan untuk pencegahan terjadinya froud dari bidang akuntansi yaitu dengan mengembangkan sistem informasi akuntansi dan optimalilisasi peran akunting.

1. **Pengembangan Sistem Informasi Akuntansi**

Dengan munculnya teknologi informasi (TI), penggunaan solusi TI untuk mendukung pengumpulan dan komunikasi informasi akuntansi harus menjadi prioritas sebagai bagian dari inisiatif untuk meningkatkan daya saing dan produktivitas

bisnis (Mitrović & Knežević, 2020; Omoteso & Obalola, 2014). Kemajuan teknologi informasi sangat mempengaruhi perkembangan sistem akuntansi perusahaan, menyebabkan penyederhanaan banyak proses, sehingga menciptakan operasi yang efisien. Aksesibilitas teknologi komputer dalam perusahaan membuka banyak peluang untuk meningkatkan usahanya. Kemajuan teknologi informasi telah membuat arus informasi menjadi efisien yang meningkatkan pengambilan keputusan manajemen, sehingga meningkatkan kemampuan bisnis untuk mencapai tujuan.

Walaupun operasi bisnis perusahaan sudah terkomputerisasi, risiko *fraud* tidak serta merta berkurang, namun juga akan menambah risiko terjadinya *fraud* yang disebabkan oleh program aplikasi itu sendiri. Risiko *fraud* yang disebabkan oleh IT dapat berupa kesalahan proses dari program, akses yang tidak sah, pencurian data, kerusakan data, dan hilangnya jejak audit.[15] Risiko ini mendorong perusahaan agar perlu mengadakan adanya kontrol yang terprogram pada sistem teknologi informasi. Untuk mengatasi risiko-risiko yang berkaitan dengan teknologi informasi, perusahaan dapat menerapkan pengendalian yang diperkenalkan oleh *Committee of Sponsoring Organization* (COSO), yaitu berupa pengendalian umum dan pengendalian aplikasi (Kim et al., 2013; Petraşcu & Tieanu, 2014). Dengan adanya kedua pengendalian tersebut, maka dapat diketahui bagaimana teknologi informasi berkontribusi terhadap kecurangan akuntansi (*fraud*) sekaligus sebagai sarana mengevaluasi pengendalian internal yang bertujuan untuk menciptakan efektivitas dan efisiensi operasi bisnis dan keandalan informasi.

Selain itu banyak lagi teknologi yang dapat digunakan untuk membantu akunting dalam memproses data. Perkembangan teknologi di bidang akuntansi saat ini tengah mengalami berbagai macam perkembangan, di antaranya ada beberapa macam teknologi informasi yaitu *Electronic Data Processing System*, *Data Processing System* (DPS), *Decisions Support System* (DSS), *Management Information System* (MIS), *Executive Information System* (EIS), *Expert System* (ES), *Accounting Information System* (AIS), dan masih banyak lagi(Demirović et al., 2021; Maruta, 2016). Teknologi tersebut dengan mudah mengolah ratusan bahkan jutaan data-data serta informasi yang dibutuhkan oleh para akuntan di zaman modern ini.

Perlu diingat bahwa teknologi informasi yang diterapkan dalam akuntansi tidaklah "sempurna". Berkenaan dengan sistem informasi akuntansi perusahaan, sistem ini sangat membantu dalam proses akuntansi. Namun, kita perlu mempertimbangkan kemungkinan bahwa sistem terkadang menjadi tidak efisien, seperti yang terjadi pada beberapa perangkat lunak akuntansi. Saat ini, teknologi informasi telah meningkatkan proses akuntansi, tetapi

komputer masih belum dapat menggantikan peran manusia dalam sistem akuntansi (Maruta, 2016).

Dalam menghindari potensi kerugian yang lebih besar, perusahaan bisa menetapkan jumlah limit yang dapat digunakan untuk membatasi bertransaksi. Saat transaksi melebihi limit yang ditetapkan maka transaksi tersebut otomatis ditolak. Hal ini akan membatasi tingkat kerugian yang dialami perusahaan jika terjadi *fraud* kartu kredit.

Adapun pencatatan kerugian perusahaan akibat terjadinya tindak kejahatan *fraud* ini dicatat sebagai biaya pada laporan laba-rugi (*income statement*) dan bukan pada penghasilan komprehensif lain (*other comprehensive income atau OCI*) yang walaupun kerugian ini bukan dari aktivitas utama perusahaan namun menimbang OCI umumnya terdiri dari 2 kategori yaitu yang tidak akan direklasifikasikan ke laporan *income statement* seperti revaluasi aset tetap dan aset takberwujud; program imbalan pasti (PSAK 24) dan yang akan direklasifikasikan ke laporan *income statement* seperti keuntungan atau kerugian dari aktivitas keuangan entitas asing; revaluasi aset keuangan (bisa berupa obligasi dan saham) yang siap untuk dijual; keuntungan atau kerugian dari lindung nilai (*hedge*). Diluar 5 aktivitas ini, dimasukan ke dalam laporan *income statement*.

Dari sisi perpajakan, kerugian atas *fraud* ini akan dilakukan koreksi positif saat perhitungan Pajak Penghasilan Badan Tahunan (PPh Badan) karena dianggap bukan merupakan biaya yang dapat dikurangkan dalam menentukan besarnya penghasilan kena pajak sesuai dengan pasal 6 UU Pajak Penghasilan tahun 2008 karena bukan termasuk biaya untuk mendapatkan, menagih, dan memelihara penghasilan. Akibat kerugian *fraud* ini menyebabkan pajak penghasilan yang lebih tinggi.

2. Optimalisasi Peran Akuntan

Dengan kemajuan teknologi saat ini, perusahaan dapat menerbitkan kartu kredit atau kartu kredit yang dipercayakan kepada karyawan tertentu, tetapi ada risiko dengan keputusan itu, seperti karyawan yang menggunakan kartu tersebut untuk pengeluaran pribadi. Tidak dipungkiri kartu kredit, kartu debit, dan tagihan membuat arus perdagangan lebih lancar dan nyaman, tetapi ada resiko tersendiri didalamnya. Untuk itu dari bidang akuntasi diperlukan cara melindungi bisnis dari penipuan kartu kredit melalui penggunaan kontrol internal yang tepat.

Salah satu pihak yang memiliki peran sebagai pengendali internal pada kegiatan perekonomian dalam perusahaan yaitu para akuntan yang hampir setiap waktu berhubungan dengan teknologi informasi (Hazami-Ammar, 2019; Omoteso & Obalola, 2014). Selain itu, peran akuntan dalam perencanaan dan penilaian risiko menurut ISA 315.14 bahwa auditor harus memperoleh pemahaman tentang lingkungan

pengendalian, Know Your Customer (KYC) yang meningkatkan dokumentasi vendor atau pemasok, dan memastikan alokasi sumber daya untuk biaya keamanan siber waktu dan uang. Tapi kurangnya perlindungan bisa lebih mahal.

Sistem pengendalian intern meliputi struktur organisasi, metode dan ukuran-ukuran yang dikoordinasikan untuk menjaga kekayaan organisasi, mengecek ketelitian dan dapat dipercaya tidaknya data akuntansi mendorong efisiensi dan mendorong dipatuhinya kebijaksanaan.[20]

Berdasarkan lingkupnya, pengendalian internal dibedakan menjadi:

a. Pengendalian akuntansi yang berfungsi untuk mengamankan sumber daya organisasi dari penyalahgunaan dan menjaga kecermatan data akuntansi.
b. Pengendalian administratif yang berfungsi mendorong efisiensi operasi dan mengupayakanagar kebijakan ataupun tujuan manajemen dapat tercapai.

Apabila ditinjau dari terjadinya permasalahan yang harus dikendalikan, pengendalian internal dapat dibedakan menjadi:

a. Pengendalian preventif atau pengendalian umpan maju, yaitu pengendalian dengan jalan menangkal sebelum permasalahan terjadi dan untuk mencegah terjadinya ketidakefisienan.
b. Pengendalian detektif atau umpan balik, yaitu pengendalian yang berfungsi mengungkap permasalahan dalam suatu aktivitas, segera setelah aktivitas itu terjadi.
c. Pengendalian korektif adalah pengendalian yang berfungsi mengoreksi kesalahan yang ditemukan oleh pengendalian detektif.

Pengendalian internal juga diklsifikasikan menjadi pengendalian umum dan pengendalian aplikasi. Pengendalian umum adalah pengendalian yang dirancang agar lingkungan pengendalian organisasi menjadi stabil dan terkelola dengan baik sehingga dapat mendukung efektifitas pengendalian aplikasi. Sedangkan pengendalian aplikasi adalah pengendalian yang digunakan untuk mencegah, mendeteksi, dan memperbaiki kesalahan serta penyimpangan dalam transaksi pada saat diproses. Lebih lanjut sistem pengendalian internal juga dapat diklasifikasikan ke dalam pengendalian input, pengendalian proses, dan pengendalian output. Pengendalian input yaitu pengendalian yang dirancang untuk menjaga agar data yang dimasukkan ke dalam sistem adalah data yang akurat, valid, dan telah diotorisasi oleh pihak yang berwenang. Pengendalian proses adalah pengendalian yang dirancang untuk menjaga agar semua transaksi diproses secara akurat dan lengkap, sehingga semua arsip dan catatan dapat dimutkhirkan dengan baik. Pengendalian output merupakan bentuk pengendalian yang dirancang untuk menjaga agar output sistem dapat dikendalikan dengan baik.

Apapun bentuk klasifikasi dari sistem pengendalian internal, semuanya memiliki tujuan yang sama yaitu menjaga aktiva organisasi, memastikan akurasi dan keandalan catatan serta informasi akuntansi, mendorong efisiensi dalam operasional organisasi, dan mengukur kesesuaian dengan kebijakan serta prosedur yang ditetapkan oleh pihak manajemen.

Dari adanya fungsi pengendalian yang dimiliki akuntan dalam organisasi menunjukkan bahwa para akuntan memiliki peran yang cukup krusial dalam meminimalkan tindak kejahatan *Cybercrime*, seperti yang dipaparkan pada *The Future of Accounting: New Frontiers, Technology, and Cybersecurity*" menjelaskan bahwasanya peranan akuntan sangat dibutuhkan dalam mereduksi tindak kriminal tersebut. secara eksternal perusahaan tidak selalu memiliki sumber daya (waktu, tenaga, uang, dan keahlian) untuk menjadi yang terbaik dalam pencegahan kejahatan siber (Aseri & Gera, 2014; Maruta, 2016; Setiawan, 2019).

Potensi kejahatan siber khususnya pada *fraud* kartu kredit dan kartu debit dapat terjadi didalam perusahaan. Pelaku kejahatan tersebut tidak dipungkiri dapat dilakukan oleh orang dalam perusahaan sendiri. Pencegahan tindakan *fraud* kartu kredit dan kartu debit dalam perusahaan dapat dilakukan dengan meningkatkan peran akuntan dalam perusahaan. Dimana tidak hanya mengawasi, menghitung, dan membuat laporan keuangan sebuah instansi, perusahaan, atau lembaga tempatnya bekerja, namun juga harus mampu membaca karakteristik perilaku manusia dalam perusahaan. Seorang akuntan professional harus dapat memanfaatkan berbagai kemajuan teknologi dan wawasan ilmiah. Hal tersebut diperlukan untuk melawan penipuan dan memulihkan kepercayaan dalam laporan keuangan, melalui pemeriksaan dan interpretasi bukti dan fakta dan penilaian ahli atas dasar itu.

Untuk mengoptimalkan keahlian seorang profesional akuntan yang terlatih dan berpengalaman menjadi penyelidik keuangan yang baik yang terpenting adalah pengetahuan tentang perilaku manusia, kepekaan seorang akuntan untuk mengetahui setiap tanda bahaya dan rasa intuitif yang baik tentang pentingnya bukti. Akuntan yang profesional harus memiliki pendekatan interdisipliner untuk menjelaskan berbagai masalah, dan karena itu menggunakan pengetahuan akuntansi, audit dan investigasi (Tugiman, 2006).

Profesional akuntan memainkan dua peran penting dalam setiap penyelidikan *fraud* dalam perusahaan yaitu sebagai penyelidik keuangan dan, berpotensi, sebagai saksi ahli dalam persidangan perdata atau pidana. Dalam peran pertama, akuntan mewakili tokoh kunci dalam setiap penyelidikan penipuan, karena mereka mengetahui sistem akuntansi dan kontrol internal dan tahu bagaimana melacak aliran aset di dalam, melalui dan di luar perusahaan.

Akuntan juga memiliki posisi untuk memberikan kritik yang independen dan objektif terhadap perusahaan. Kritik tersebut tidak hanya mencakup masalah dalam sistem akuntansi yang memungkinkan terjadinya penipuan sejak awal, tetapi juga membahas integritas orang-orang yang terlibat dalam proses *fraud* tersebut. Sebagai ahli dalam membantu strategi kasus dan kesaksian, profesional akuntansi mengetahui aturan pembuktian, dokumen apa yang harus dicari, siapa yang harus diajak bicara, dan banyak lagi (Maruta, 2016). Dan kedua, seorang akuntan juga berperan untuk mengumpulkan bukti dengan tujuan membentuk opini, yang umumnya disajikan sebagai bukti ahli di pengadilan. Oleh karena itu akuntan harus memiliki kompetensi profesional, kehati-hatian, perencanaan dan pengawasan dan informasi relevan yang memadai.

Pembatasan jumlah limit penggunaan kartu kredit juga merupakan satu bentuk pengendalian internal. Akuntan segera melakukan pembukuan atas semua transaksi dalam tagihan kartu kredit dan jika ada transaksi ternyata tidak dilakukan oleh pemegang kartu kredit maka bisa segera melakukan tindakan pemblokiran kartu kredit karena ada indikasi kartu kredit tersebut sudah bobol dan dipakai oleh orang lain untuk melakukan tindak kejahatan *fraud* kartu kredit. Pelaporan atas transaksi ini kepada pihak bank yang mengeluarkan kartu kredit dan kepada pihak yang berwajibdalam hal ini kepolisian, perlu dilakukan agar pihak yang terkait bisa melakukan tindakan yang diperlukan baik untuk mencegah hal ini terjadi lagi maupun untuk menangkap oknum yang melakukan tindakan kejahatan ini.

KESIMPULAN

Tindak kejahatan *cyber* khususnya *credit/debit card fraud* tidak hanya merugikan individu, namun juga dapat berdampak pada perusahaan. Karakter tindak pidana *credit / debit card fraud* bahwa tindak pidana tersebut, selalu terdiri dari, minimal, dua tindakan, yaitu pertama adalah *identity theft* (pencurian identitas), dan kedua penggunaan transaksi. Transaksi berbasis kartudapat diklasifikasikan menjadi dua jenis. Pertama, transaksi menggunakan kartu kredit dalam bentuk fisik, dan kedua transaksi kartu jarak jauh. Skema *card fraud* diantaranya Pelaku menggunakan kartu kredit (dalam bentuk fisik) asli untuk digunakan transaksi dan/atau pelaku menggunakan data elektronik terkait kartu kredit seperti nomor kartu kredit, nama pemegang, nama penerbit, tanggal kadaluarsa, kode pengaman, dan nomer varifikasi kartu kredit (CVV: *Card Verification Value*) untuk berbelanja.

Beberapa upaya yang dilakukan untuk pencegahan terjadinya *fraud* dari bidang akuntansi yaitu dengan mengembangkan sistem informasi akuntansi dan optimalilisasi peran akunting. Pencegahan tindakan *fraud* kartu kredit dan kartudebit dalam perusahaan dapat dilakukan dengan meningkatkan peran akuntan dalam perusahaan. Dimana tidak

hanya mengawasi, menghitung, dan membuat laporan keuangan sebuah instansi, perusahaan, atau lembaga tempatnya bekerja, namun juga harus mampu membaca karakteristik perilaku manusia dalam perusahaan. Seorang akuntan professional harus dapat memanfaatkan berbagai kemajuan teknologi dan wawasan ilmiah. Hal tersebut diperlukan untuk melawan penipuan dan memulihkan kepercayaan dalam laporan keuangan, melalui pemeriksaan dan interpretasi bukti dan fakta dan penilaian ahli atas dasar itu

DAFTAR PUSTAKA

Adepoju, O., Wosowei, J., & Jaiman, H. (2019). Comparative evaluation of credit card fraud detection using machine learning techniques. In 2019 Global Conference for Advancement in Technology (GCAT), 1-6 IEEE.

Apriwandi, & Supriyono, R. A. (2021). Actual participation: The effects of information sharing and familiarity team on budget decision quality. International Journal of Monetary Economics and Finance, 14(2), 188–195. https://doi.org/10.1504/IJMEF.2021.114025

Arens Alvin A, Elder Randal J, Beasley Mark S, A. A. J. (2015). Auditing dan Jasa Assurance (E. Keduabelas (ed.)). Salemba empat.

Aseri, E. K., & Gera, O. P. (2014). Current Trends Of It And Cyber Security. Horizon Books, 124.

Chaudhary. (2012). Credit Card Fraud: The study of its impact and detection. International Journal of Computer Science and Network (IJCSN), 1(4).

Christine, D., & Apriwandi. (2022). Audit Internal dan Pencegahan Kecurangan-Bukti Empiris Pada Badan Urusan Logistik (BULOG). Owner: Riset & Jurnal Akuntansi, 6, 3270–3280.

Deloitte. (2013). Financial crime survey report 2013:where is the exposure?"; available at: http://; Deloitte_Financial_Crimes_Survey_Report-2013.pdf (.

Demirović, L., Isaković-Kaplan, Š., & Proho, M. (2021). Internal Audit Risk Assessment in the Function of Fraud Detection. Journal of Forensic Accounting Profession, 1(1), 35–49. https://doi.org/10.2478/jfap-2021-0003

Dornadula, V. N., & Geetha, S. (2019). Credit card fraud detection using machine learning algorithms. Procedia Computer Science, 165, 631–641.

Fullerton, R., & Durtschi, C. (2011). The Effect of Professional Skepticism on the Fraud Detection Skills of Internal Auditors. SSRN Electronic Journal, 435. https://doi.org/10.2139/ssrn.617062

Ghozali, I. (2011). Aplikasi Analisis Multivariate Dengan Program SPSS. Semarang: Badan Penerbit Universitas Dipenogoro.

Gunadi, E. M. (2001). Prevention and Detection of Fraud a Challenge to the Internal Auditors. Kriminologi Indonesia, 1(III), 43–49.

Hazami-Ammar, S. (2019). Internal auditors' perceptions of the function's ability to investigate fraud. Journal of Applied Accounting Research, 20(2), 134–153. https://doi.org/10.1108/JAAR-09-2017-0098

Hille, G, W., & M, C. (2016). Consumer Fear of Online Identity Theft: Scale

Development and Validation. Journal of Interactive Marketing, 30(1), 1–17.

Jogiyanto Hartono. (2015). Metodologi Penelitian Bisnis Salah Kaprah dan Pengalaman (B. U. G. Mada (ed.)).

Kim, T. K., Lim, H. J., & Nah, J. H. (2013). Analysis on fraud detection for internet service. International Journal of Security and Its Applications, 7(6), 275–284.

Maruta, H. (2016). Pengendalian Internal Dalam Sistem Informasi Akuntansi. Jurnal Ilmiah Ekonomi Kita, 5(1), 16–28.

Mitrović, A., & Knežević, S. (2020). Fraud And Forensic Accounting In The Digital Environment Of Accounting Information Systems: Focus On The Hotel Industry. In Tourism International Scientific Conference Vrnjačka Banja-TISC, 5(1).

Omoteso, K., & Obalola, M. (2014). The Role of Auditing in the Management of Corporate Fraud. 129–151. https://doi.org/10.1108/s2043-052320140000006006

Petraşcu, D., & Tieanu, A. (2014). The Role of Internal Audit in Fraud Prevention and Detection. Procedia Economics and Finance, 16(May), 489–497. https://doi.org/10.1016/s2212-5671(14)00829-6

Said Noor Prasetyo. (2016). Rumusan Pengaturan Credit Card Fraud Dalam Hukum Pidana Indonesia Ditinjau Dari Asas Legalitas. Jurnal Legality, 24(1), 101–119.

Saragih, M. G., Chin, J., Setyawasih, R., Nguyen, P. T., & Shankar, K. (2019). Machine learning methods for analysis fraud credit card transaction. International Journal of Engineering and Advanced Technology (IJEAT).

Setiawan, D. A. (2019). Perkembangan Modus Operandi Kejahatan Skimming Dalam Pembobolan Mesin Atm Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybercrime). Era Hukum-Jurnal Ilmiah Ilmu Hukum, 6(1).

Tugiman, H. (2006). Standart Profesional Audit Internal. Yogyakarta: Kanisius.

Vaswani, M. (1997). Journal of Financial Crime. Journal of Financial Crime Iss, 5(1), 39–44.