Jurnal Multidisiplin Indonesia (JOUMI)
Volume 4 Nomor 2 Juni 2026

E-ISSN .: 2986-7541; P-ISSN .: 2986-7533, Hal 166-178
DOI: https://doi.org/10.62007/joumi.v4i2.654
Tersedia : https://ejournal.alhafiindonesia.co.id/index.php/JOUMI

Dibalik Bukti Pembayaran: Analisis Literatur atas Kelemahan Sistem dalam Modus Billing dan Disbursement Fraud

Anesta Wahyuni
Program Studi Magister Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Islam Bandung, Indonesia
Pupung Purnamasari
Program Studi Magister Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Islam Bandung, Indonesia
Email: [1] anestawahyuni03@gmail.com
[2] pupung@unisba.ac.id

Korespondensi penulis: anestawahyuni03@gmail.com

Abstract. *The emergence of digital financial technology has led to the emergence of new forms of economic crime, particularly fraudulent collection and disbursement schemes. These crimes involve the manipulation of payment documents, such as fake invoices, mark-up schemes, split invoices, and fake transfer receipts. This study uses a qualitative case study approach to analyze ten real-life cases from Indonesia and abroad, revealing common vulnerabilities in digital transaction systems, including the absence of real-time verification, low financial literacy, and weak internal controls. Applying the Fraud Triangle theory, this study highlights "opportunity" as the dominant factor enabling fraudulent activities. The findings highlight the need for real-time notification systems, increased digital literacy, the application of artificial intelligence to detect fraud, and stronger financial governance. This study contributes to the understanding of how fraudulent transactions are conducted and offers practical recommendations for prevention in the digital economy.*

Keywords: *digital fraud, transfer receipt manipulation, fake invoices, digital crime prevention, fraud triangle*

Abstrak. Munculnya teknologi keuangan digital telah menyebabkan munculnya bentuk-bentuk kejahatan ekonomi baru, khususnya penipuan penagihan dan pencairan dana. Kejahatan ini melibatkan manipulasi dokumen pembayaran, seperti faktur palsu, skema mark-up, faktur terpisah, dan bukti transfer palsu. Studi ini menggunakan pendekatan studi kasus kualitatif untuk menganalisis sepuluh kasus nyata dari Indonesia dan luar negeri, yang mengungkap kerentanan umum dalam sistem transaksi digital, termasuk tidak adanya verifikasi waktu nyata, literasi keuangan yang rendah, dan kontrol internal yang lemah. Dengan menerapkan teori Segitiga Penipuan, studi ini menyoroti "peluang" sebagai faktor dominan yang memungkinkan terjadinya penipuan. Temuan menekankan perlunya sistem pemberitahuan waktu nyata, peningkatan literasi digital, adopsi kecerdasan buatan untuk deteksi penipuan, dan tata kelola keuangan yang lebih kuat. Studi ini berkontribusi pada pemahaman bagaimana transaksi curang dilakukan dan menawarkan rekomendasi praktis untuk pencegahan dalam ekonomi digital.

Kata Kunci: penipuan digital, manipulasi bukti transfer, faktur palsu, pencegahan kejatahan digital, segitiga penipuan

Received Juni 03, 2026; Revised Juni 12, 2026; Juni 22, 2026
*Corresponding author, e-mail address : anestawahyuni03@gmail.com

PENDAHULUAN

Perkembangan teknologi informasi dan sistem keuangan digital telah mendorong munculnya bentuk-bentuk baru kejahatan ekonomi yang memanfaatkan kelemahan dalam sistem administrasi keuangan. Salah satu bentuk kejahatan tersebut adalah billing fraud dan disbursement fraud, yakni penipuan yang dilakukan melalui manipulasi dokumen pembayaran, seperti invoice fiktif, split invoice, mark-up biaya, hingga bukti transfer yang dipalsukan. Sistem dalam konteks ini merujuk pada prosedur, pengawasan, dan infrastruktur digital yang digunakan dalam pencatatan, verifikasi, dan otorisasi transaksi keuangan. Ketika sistem tersebut memiliki celah, maka pelaku dapat menyalahgunakannya untuk memperoleh keuntungan pribadi secara tidak sah.

Istilah "dibalik bukti pembayaran" mengacu pada fakta bahwa di balik tampilan dokumen atau bukti transaksi yang terlihat sah, sering tersembunyi rekayasa yang disengaja untuk menipu pihak lain. Bukti transfer, invoice, atau struk QRIS yang secara visual tampak valid seringkali hanyalah manipulasi digital yang digunakan untuk membangun kepercayaan palsu. Oleh karena itu, analisis terhadap sistem dan prosedur di balik bukti pembayaran menjadi penting untuk mengungkap bagaimana penipuan ini dapat terjadi dan berkembang.

Fenomena meningkatnya kasus kejahatan ekonomi digital dapat terlihat dari sepuluh kasus nyata yang dianalisis dalam penelitian ini. Pada kategori disbursement fraud, ditemukan modus seperti penggunaan bukti transfer palsu saat bertransaksi secara langsung maupun daring, baik melalui tangkapan layar yang dimanipulasi, aplikasi palsu, hingga penyalahgunaan sistem QRIS tanpa adanya transaksi riil. Kasus-kasus seperti yang terjadi di pusat perbelanjaan Jakarta Selatan dan di kota Makassar menunjukkan bahwa pelaku mampu menyakinkan korban dengan tampilan bukti pembayaran yang tampak sah. Bahkan dalam konteks QRIS, tidak sedikit pedagang yang tertipu karena tidak menerima notifikasi, padahal pembeli telah menunjukkan "struk" palsu.

Sementara itu, pada kategori billing fraud, modus yang ditemukan melibatkan penyusunan invoice fiktif, penggelembungan nilai invoice (*mark-up*), serta split invoice. Contohnya adalah kasus restoran di Bali yang ditipu turis asing dengan bukti transfer fiktif yang terlampir dalam invoice, dan dugaan manipulasi pengadaan oleh PLN ULP Ambunten serta proyek BTS 4G. Selain itu, di tingkat internasional, ditemukan pula modus duplikasi cek menggunakan mobile deposit yang menandakan kerentanan dalam sistem pencairan dana.

Kesamaan dari semua kasus tersebut adalah manipulasi terhadap dokumen atau bukti pembayaran yang seolah-olah valid, namun menyimpan rekayasa penipuan di baliknya. Hal ini menegaskan bahwa sistem administrasi dan verifikasi transaksi masih memiliki celah yang dapat dimanfaatkan. Dibalik bukti pembayaran yang tampak sah, tersimpan ancaman serius terhadap keamanan sistem keuangan digital. Oleh karena itu, penting dilakukan analisis kritis terhadap bagaimana sistem bekerja, di mana titik lemahnya, dan strategi apa yang dapat digunakan untuk menutup celah tersebut.

Hal ini menciptakan research gap yang perlu diteliti secara mendalam untuk merumuskan strategi pencegahan dan perlindungan terhadap konsumen maupun pelaku usaha.

Penelitian ini mengacu pada teori Fraud Triangle dari Donald Cressey yang menjelaskan bahwa fraud terjadi karena adanya tekanan (*pressure*), peluang (*opportunity*), dan rasionalisasi (*rationalization*). Dalam konteks kejahatan digital, peluang menjadi faktor dominan karena lemahnya kontrol sistem, minimnya literasi keuangan digital, serta tidak adanya verifikasi berlapis dalam proses transaksi. Penelitian ini memiliki kekhasan karena membahas secara komprehensif lima tipe kejahatan digital dan menyajikan data berbasis kasus di Indonesia dan luar negeri, serta menghubungkannya dengan teori dan kebijakan terkini.

KAJIAN TEORI

2.1 Fraud Triangle Theory

Teori Fraud Triangle yang dikembangkan oleh Donald Cressey menjadi dasar utama dalam memahami bagaimana dan mengapa seseorang melakukan fraud. Teori ini menyatakan bahwa fraud terjadi ketika tiga elemen utama hadir, yaitu tekanan (*pressure*), peluang (*opportunity*), dan rasionalisasi (*rationalization*). Tekanan dapat berasal dari kebutuhan ekonomi, tuntutan gaya hidup, atau kondisi psikologis tertentu yang memotivasi individu untuk melakukan kecurangan.

Peluang muncul ketika individu melihat adanya kelemahan dalam sistem pengendalian internal, kurangnya pengawasan, atau ketidaktahuan pihak lain terhadap aktivitas mencurigakan. Dalam konteks sistem digital, peluang ini meningkat karena sistem yang belum terintegrasi, tidak adanya verifikasi otomatis, atau sistem yang belum dilengkapi autentikasi ganda. Oleh karena itu, sistem keuangan digital rentan terhadap manipulasi seperti bukti transfer palsu, QRIS tanpa transaksi, dan invoice fiktif.

Rasionalisasi adalah pembenaran yang dibuat oleh pelaku untuk menjustifikasi tindakannya, misalnya merasa bahwa tindakannya hanyalah "meminjam" uang, atau karena merasa sistem yang digunakan memang sudah tidak adil. Ketiga elemen ini jika hadir bersamaan dapat menciptakan kondisi ideal terjadinya fraud, terlebih dalam ekosistem digital yang belum sepenuhnya memiliki kontrol ketat dan edukasi menyeluruh.

2.2 Tipologi Kejahatan Ekonomi Digital

Menurut ACFE (2023), terdapat beberapa bentuk kejahatan berbasis digital yang sering terjadi, yaitu:

- Pemalsuan bukti transfer
- Penggunaan QRIS palsu
- Penerbitan invoice fiktif
- Duplikasi cek
- Split invoice dan mark-up biaya

Kejahatan tersebut biasanya dilakukan oleh individu maupun kelompok yang memanfaatkan kelemahan sistem transaksi elektronik dan kurangnya pengawasan pada sistem pembayaran. Dalam konteks perusahaan, kejahatan ini juga sering ditemukan pada proses pengadaan barang dan jasa yang tidak transparan.

2.3 Penelitian Terdahulu

Azizah & Rahmadani (2022) dalam penelitiannya berjudul "Analisis Penipuan QRIS dan Perlindungan Konsumen" menyebutkan bahwa banyaknya kasus penipuan QRIS disebabkan oleh lemahnya sistem notifikasi yang tidak terintegrasi dengan kasir merchant secara real-time. Mereka menyarankan penguatan teknologi notifikasi QRIS dan kontrol dari regulator agar QRIS tidak dapat dipalsukan dengan tangkapan layar atau aplikasi edit.

Rahmanti & Widodo (2023) dalam jurnalnya mengenai penipuan transaksi digital menemukan bahwa bukti transfer palsu menjadi metode dominan penipuan dalam platform jual beli online. Mereka mencatat bahwa pelaku umumnya menggunakan aplikasi edit bukti transfer dan mengirimkan dokumen ke penjual sebelum dana benar-benar diterima. Penelitian ini menekankan pentingnya verifikasi otomatis dari sistem pembayaran yang terintegrasi dengan dashboard merchant.

Wijayanti (2023) melakukan penelitian mengenai sistem audit digital dalam mendeteksi invoice fiktif, terutama di sektor pengadaan pemerintah daerah. Ia menemukan bahwa ketiadaan verifikasi elektronik pada sistem pengadaan memungkinkan adanya pembuatan invoice fiktif yang

disetujui secara manual oleh oknum. Penelitian ini merekomendasikan implementasi e-budgeting dan digital audit trail untuk menutup celah kecurangan administratif tersebut.

2.4 Hipotesis Pengembangan

Jika penelitian ini dilanjutkan dalam format kuantitatif, maka hipotesis yang dapat dibangun adalah: "Semakin tinggi kompleksitas sistem digital yang tidak didukung oleh kontrol internal yang kuat, maka semakin besar potensi terjadinya fraud digital."

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus. Fokus utama adalah menganalisis kasus-kasus penipuan digital di Indonesia dan luar negeri berdasarkan berita-berita aktual serta didukung oleh teori dan penelitian terdahulu. Studi ini bertujuan untuk mengeksplorasi secara mendalam modus operandi, faktor penyebab, pencegahan, serta penyelesaian dari setiap jenis fraud digital.

3.1 Jenis Penelitian

Jenis penelitian ini adalah penelitian kualitatif eksploratif. Pendekatan ini dipilih karena kasus fraud digital bersifat kompleks, kontekstual, dan dinamis, sehingga memerlukan pemahaman mendalam terhadap pola perilaku pelaku, sistem yang disalahgunakan, serta proses penyelesaian yang dilakukan.

3.2 Obyek dan Sumber Data

Objek dalam penelitian ini adalah berbagai kasus fraud digital yang terjadi selama tahun 2023–2024 dengan fokus pada lima kategori utama, yaitu: pemalsuan bukti transfer, QRIS palsu, invoice fiktif, duplikasi cek, dan split invoice. Sumber data berupa data sekunder yang diperoleh dari berita-berita online terpercaya seperti Detik.com, Kompas.com, Republika, Radar Lombok, serta dokumen-dokumen resmi dari instansi pemerintah dan lembaga hukum internasional (US DOJ).

3.3 Teknik Pengumpulan Data

Data dikumpulkan melalui studi pustaka dan studi dokumentasi. Sepuluh artikel berita dianalisis secara sistematis berdasarkan klasifikasi bentuk penipuan, pelaku, kronologi kejadian, metode penipuan yang digunakan, serta langkah penegakan hukum yang diambil. Peneliti juga menelusuri literatur akademik dan kebijakan yang relevan sebagai pelengkap analisis.

3.4 Teknik Analisis Data

Teknik analisis yang digunakan adalah analisis konten dan tematik. Setiap kasus dianalisis berdasarkan:

- Overview Kasus: Latar belakang dan gambaran umum kasus
- Modus Operandi: Teknik dan alat yang digunakan pelaku
- Faktor Penyebab: Sistem, kelemahan teknologi, atau perilaku manusia
- Pencegahan: Langkah preventif yang seharusnya dilakukan
- Penyelesaian: Tindakan yang diambil oleh korban atau aparat hukum

Analisis ini dikaitkan dengan teori Fraud Triangle dan temuan dari penelitian terdahulu, untuk membangun pemahaman yang komprehensif mengenai dinamika kejahatan digital.

HASIL DAN PEMBAHASAN

4.1 Kasus 1: Pemalsuan Bukti Transfer - Kasus Wanita di Mal Jakarta Selatan

a) Overview Kasus: Seorang wanita viral karena diduga memalsukan bukti transfer saat berbelanja di sebuah mal di Jakarta Selatan. Ia menunjukkan bukti transfer kepada kasir, namun uang tidak masuk ke rekening tujuan.
b) Modus Operandi: Pelaku diduga menggunakan aplikasi edit gambar atau fitur di ponsel untuk membuat tampilan seolah-olah telah terjadi transfer. Bukti tersebut kemudian dikirim ke kasir sebagai konfirmasi palsu.
c) Faktor Penyebab: Tidak adanya sistem verifikasi otomatis antar merchant dengan sistem bank atau tidak ada sinkronisasi real-time.
d) Pencegahan: Implementasi sistem notifikasi transaksi real-time dan pelatihan pegawai untuk memverifikasi transfer melalui dashboard resmi merchant.
e) Penyelesaian: Polisi melakukan penyelidikan setelah laporan viral. Penegakan hukum masih dalam proses.

4.2 Kasus 2: Pembelian HP Menggunakan Bukti Transfer Palsu di Makassar

a) Overview Kasus: Dua pelaku membeli HP dari toko dengan menunjukkan bukti transfer palsu dan berhasil membawa barang sebelum dana benar-benar masuk ke rekening penjual.
b) Modus Operandi: Mereka memanfaatkan kepercayaan penjual dan memberikan screenshot transfer palsu. Salah satu pelaku mengaku mentransfer dari mobile banking.
c) Faktor Penyebab: Penjual tidak menunggu notifikasi masuk dana dan sistem POS tidak terkoneksi ke rekening.

d) Pencegahan: Prosedur wajib menunggu bukti dana masuk, penggunaan QRIS atau EDC bank dengan sistem validasi otomatis.
e) Penyelesaian: Polisi menangkap pelaku setelah pelaporan korban dan menyita barang bukti HP serta tangkapan layar palsu.

4.3 Kasus 3: Mahasiswi Gunakan Struk QRIS Palsu di Alun-Alun Purwokerto

a) Overview Kasus: Seorang mahasiswi diduga menggunakan struk QRIS palsu saat membeli makanan di alun-alun Purwokerto. Penjual baru menyadari tidak ada uang masuk setelah transaksi dilakukan.
b) Modus Operandi: Pelaku menunjukkan tangkapan layar struk pembayaran QRIS yang telah diedit atau diambil dari transaksi sebelumnya untuk mengelabui pedagang.
c) Faktor Penyebab: Tidak adanya notifikasi otomatis di sisi pedagang dan kurangnya pelatihan pelaku usaha kecil dalam mengenali transaksi QRIS asli.
d) Pencegahan: Penggunaan aplikasi QRIS resmi dengan sistem notifikasi langsung dan edukasi rutin kepada pelaku UMKM.
e) Penyelesaian: Kasus viral di media sosial. Polisi memberikan edukasi kepada pelaku dan pedagang untuk menghindari kejadian serupa.

4.4 Kasus 4: Penipuan QRIS Tanpa Notifikasi di Lombok

a) Overview Kasus: Banyak pedagang kecil menjadi korban penipuan QRIS palsu karena tidak mendapat notifikasi pembayaran, padahal pembeli mengaku telah mentransfer.
b) Modus Operandi: Pelaku berpura-pura mentransfer dengan aplikasi palsu atau menunjukkan bukti screenshot dari transaksi sebelumnya.
c) Faktor Penyebab: Minimnya edukasi pengguna QRIS dan tidak adanya sistem validasi otomatis di perangkat pedagang.
d) Pencegahan: Peningkatan sistem notifikasi QRIS dan penggunaan mesin EDC dengan verifikasi real-time.
e) Penyelesaian: Otoritas daerah bekerja sama dengan Bank Indonesia memberikan edukasi kepada pelaku usaha.

4.5 Kasus 5: Turis Pakistan Gunakan Bukti Transfer Fiktif di Bali

a) Overview Kasus: Seorang turis asal Pakistan makan di restoran mewah lalu menunjukkan bukti transfer palsu sebagai tanda pembayaran.
b) Modus Operandi: Pelaku membuat dokumen transfer fiktif dari aplikasi edit gambar lalu menyerahkannya ke kasir sebagai bukti pembayaran.

c) Faktor Penyebab: Tidak adanya prosedur standar verifikasi pembayaran asing dan kurangnya pelatihan staf hotel/restoran dalam menangani tamu internasional.
d) Pencegahan: SOP verifikasi pembayaran dengan validasi sistem bank dan penggunaan QRIS lintas negara.
e) Penyelesaian: Pelaku ditangkap dan dijatuhi hukuman pidana ringan sebagai bentuk efek jera.

4.6 Kasus 6: Penipuan Bukti Transfer di Yogyakarta

a) Overview Kasus: Seorang pria menipu beberapa toko di Yogyakarta dengan menunjukkan bukti transfer palsu. Ia berhasil membawa beberapa produk tanpa membayar.
b) Modus Operandi: Pelaku mengedit bukti transfer dan memanfaatkan waktu transaksi yang ramai untuk menghindari verifikasi kasir.
c) Faktor Penyebab: Kurangnya pelatihan pegawai dan tidak adanya sistem pengecekan digital.
d) Pencegahan: Pelatihan kasir dan integrasi dashboard POS dengan rekening bank untuk verifikasi otomatis.
e) Penyelesaian: Polisi mengamankan pelaku dan mengungkap jaringan pelaku lain di wilayah DIY.

4.7 Kasus 7: Duplikasi Cek oleh Sindikat Internasional

a) Overview Kasus: Enam terdakwa di AS terlibat dalam sindikat pencurian cek dan penipuan bank senilai jutaan dolar dengan menduplikasi cek dan mencairkannya secara ilegal.
b) Modus Operandi: Mereka mencuri cek fisik dari kotak surat, memalsukannya dengan scanner dan printer warna, lalu menyetorkannya ke rekening bayangan.
c) Faktor Penyebab: Sistem cek manual yang masih digunakan di AS serta lemahnya sistem pemantauan transaksi mencurigakan.
d) Pencegahan: Digitalisasi penuh proses pembayaran dan peningkatan sistem fraud detection oleh perbankan.
e) Penyelesaian: Keenam pelaku ditangkap dan didakwa dalam sistem peradilan federal AS.

4.8 Kasus 8: Duplikasi Cek di Sistem Mobile Deposit

a) Overview Kasus: Laporan menyebut peningkatan penipuan cek duplikat sejak penggunaan sistem mobile deposit meningkat di AS.
b) Modus Operandi: Pelaku menyetorkan cek secara digital dua kali ke dua rekening berbeda sebelum cek tersebut diproses penuh.
c) Faktor Penyebab: Kelemahan sistem mobile banking dalam mengenali duplikasi deposit.

d) Pencegahan: Implementasi teknologi AI dalam mendeteksi duplikasi transaksi dan edukasi kepada nasabah.

e) Penyelesaian: Bank-bank memperketat verifikasi digital dan menyempurnakan sistem blokir otomatis.

4.9 Kasus 9: Mark-Up Invoice PLN ULP Ambunten

a) Overview Kasus: PLN ULP Ambunten diduga melakukan mark-up invoice dalam proses pengadaan barang dan jasa yang memicu sorotan dari LSM lokal.
b) Modus Operandi: Penyusunan invoice dengan nilai yang dilebihkan dari realisasi barang yang dibeli, untuk memperoleh dana lebih.
c) Faktor Penyebab: Lemahnya pengawasan internal dan tidak adanya sistem audit digital real-time.
d) Pencegahan: Pelaksanaan e-procurement dengan e-budgeting yang transparan.
e) Penyelesaian: Investigasi dilakukan oleh auditor internal dan Kejaksaan Negeri Sumenep.

4.10 Kasus 10: Kontraktor Mark-Up Harga Proyek BTS 4G

a) Overview Kasus: Seorang kontraktor melakukan mark-up pengajuan harga dalam proyek BTS 4G untuk menyesuaikan fee yang harus dibayarkan.
b) Modus Operandi: Penggelembungan harga barang dalam invoice agar memperoleh margin keuntungan lebih dan membayar fee ilegal.
c) Faktor Penyebab: Praktik suap yang sistemik dan tidak adanya pembatasan harga satuan dalam sistem pengadaan.
d) Pencegahan: Standarisasi harga pengadaan dan pelibatan KPK dalam monitoring proyek pemerintah.
e) Penyelesaian: KPK menangkap dan menuntut pelaku serta menyita barang bukti pengadaan.

Perbandingan kasus :

Perbandingan Kasus Penipuan Bukti Transfer (Kasus 1 & Kasus 2)

Kasus pemalsuan bukti transfer di Jakarta Selatan (Kasus 1) dan Makassar (Kasus 2) memiliki kesamaan modus, yaitu penggunaan bukti transfer palsu dari mobile banking untuk meyakinkan kasir atau penjual agar menyerahkan barang tanpa adanya dana masuk. Dalam kedua kasus, pelaku memanfaatkan kepercayaan pegawai toko serta tidak adanya sistem verifikasi otomatis. Namun, kasus di Makassar dilakukan oleh dua pelaku dalam skema yang lebih terencana dan mengarah pada kerugian yang lebih nyata karena barang langsung dibawa. Faktor penyebab utamanya adalah

lemahnya kontrol transaksi dan kurangnya integrasi sistem POS dengan perbankan. Solusi yang disarankan mencakup pelatihan karyawan, penerapan sistem notifikasi transaksi real-time, serta penggunaan QRIS atau EDC yang telah tervalidasi.

Perbandingan Kasus Penipuan QRIS Palsu (Kasus 3 & Kasus 4)

Mahasiswi pengguna struk QRIS palsu di Purwokerto (Kasus 3) dan penipuan QRIS massal di Lombok (Kasus 4) mencerminkan modus serupa yakni manipulasi bukti pembayaran melalui QRIS. Pada kedua kasus, pelaku menunjukkan screenshot atau struk QRIS yang seolah-olah valid namun tidak menghasilkan transfer dana. Bedanya, kasus Purwokerto bersifat individual sedangkan di Lombok terjadi secara masif, menyasar pelaku UMKM yang minim edukasi. Penyebab utama adalah kurangnya notifikasi real-time dan rendahnya pemahaman pedagang terhadap sistem digital. Pencegahan difokuskan pada peningkatan literasi digital serta penggunaan perangkat QRIS resmi yang terhubung langsung ke sistem bank, agar transaksi bisa tervalidasi secara instan.

Perbandingan Kasus Penipuan Transfer oleh Warga Asing dan Domestik (Kasus 5 & Kasus 6)

Kasus turis Pakistan di Bali (Kasus 5) dan pria penipu di Yogyakarta (Kasus 6) menunjukkan pola kejahatan yang mirip, yakni menyalahgunakan bukti transfer yang telah diedit untuk memperoleh layanan atau barang tanpa membayar. Dalam kasus turis, penipuan terjadi di lingkungan restoran mewah dengan celah pada verifikasi pembayaran asing, sedangkan kasus di Yogyakarta lebih menyasar toko-toko umum di saat ramai transaksi. Kelemahan sistem yang dieksploitasi adalah tidak adanya SOP pengecekan pembayaran dan kurangnya pelatihan staf dalam mengecek bukti transaksi digital. Upaya mitigasi dapat dilakukan dengan standarisasi SOP verifikasi pembayaran lintas negara serta integrasi sistem kasir dengan dashboard bank untuk mengecek transfer secara otomatis.

Perbandingan Kasus Duplikasi Cek Manual dan Digital (Kasus 7 & Kasus 8)

Sindikat internasional pencuri cek (Kasus 7) dan kasus penipuan cek via mobile deposit (Kasus 8) menyoroti celah besar dalam sistem cek di Amerika Serikat, baik secara manual maupun digital. Keduanya mengandalkan duplikasi cek—baik dari hasil curian fisik maupun penyetoran digital ganda—yang menunjukkan lemahnya sistem pengamanan transaksi cek. Meskipun metode berbeda (pemalsuan fisik vs. penyalahgunaan sistem mobile banking), keduanya dipicu oleh lambannya pemrosesan dan kurangnya sistem deteksi duplikasi. Solusi jangka panjang meliputi digitalisasi penuh sistem pembayaran, peningkatan teknologi deteksi fraud berbasis AI, dan edukasi nasabah serta karyawan bank agar lebih waspada terhadap manipulasi dokumen keuangan.

Perbandingan Kasus Mark-Up Invoice Proyek (Kasus 9 & Kasus 10)

Mark-up invoice oleh PLN ULP Ambunten (Kasus 9) dan kontraktor BTS 4G (Kasus 10) sama-sama menunjukkan modus penyalahgunaan anggaran melalui penggelembungan nilai transaksi dalam invoice. Pada PLN, mark-up dilakukan dalam pengadaan rutin dan diketahui oleh LSM, sedangkan kasus BTS 4G berskala nasional dengan keterlibatan fee ilegal yang lebih sistemik dan

menyeret banyak pihak. Kedua kasus dipicu oleh lemahnya sistem audit dan kurangnya transparansi harga satuan dalam proses pengadaan. Upaya pencegahan diarahkan pada digitalisasi e-procurement, penerapan sistem harga satuan maksimal, serta pelibatan lembaga pengawas seperti BPK dan KPK dalam setiap tahapan proyek.

KESIMPULAN

Berdasarkan analisis terhadap sepuluh kasus penipuan berbasis digital, dapat disimpulkan bahwa kejahatan ini terus berkembang seiring kemajuan teknologi finansial dan lemahnya sistem pengendalian internal. Modus yang digunakan pelaku sangat variatif, mulai dari bukti transfer palsu, penggunaan QRIS palsu, invoice fiktif, hingga duplikasi cek dan mark-up pembayaran. Faktor penyebab utama antara lain adalah tidak adanya sistem verifikasi otomatis, lemahnya edukasi pelaku usaha, serta celah dalam sistem pengadaan dan pengawasan.

Untuk mencegah dan menanggulangi kejahatan ini, diperlukan kolaborasi antara pelaku usaha, otoritas keuangan, aparat penegak hukum, dan penyedia teknologi pembayaran. Peningkatan sistem notifikasi real-time, edukasi digital, digitalisasi pengadaan, dan pemanfaatan teknologi AI merupakan langkah-langkah strategis yang mendesak. Penelitian ini menyadari keterbatasan karena hanya bersumber dari data sekunder dan tidak melakukan observasi langsung, sehingga di masa depan, riset lebih mendalam melalui pendekatan lapangan dapat memperkuat validitas temuan.

DAFTAR PUSTAKA

Azizah, R. & Rahmadani, S. (2022). Analisis Penipuan QRIS dan Perlindungan Konsumen. Jurnal Manajemen dan Keuangan, 8(1), 77-89.

Rahmanti, N. & Widodo, A. (2023). Penipuan Transaksi Digital pada Platform Marketplace. Jurnal Keuangan Digital, 10(2), 131–144.

Wijayanti, R. (2023). Audit Digital untuk Deteksi Invoice Fiktif pada Sektor Pemerintahan. Jurnal Akuntansi Publik, 5(3), 202–214.

Kompas.com. (2024). Mahasiswi Pakai Struk QRIS Palsu untuk Bayar Jajan di Alun-alun Purwokerto. https://regional.kompas.com/read/2024/05/27/155743378/mahasiswi-pakai-struk-qris-palsu-untuk-bayar-jajan-di-alun-alun-purwokerto

RadarLombok.co.id. (2024). Transaksi QRIS Tanpa Notifikasi Jadi Sasaran Penipuan. https://radarlombok.co.id/transaksi-qris-tanpa-notifikasi-jadi-sasaran-penipuan.html

Detik.com. (2024). Viral Wanita Diduga Palsukan Bukti Transfer di Mal Jaksel. https://news.detik.com/berita/d-7872275/viral-wanita-diduga-palsukan-bukti-transfer-di-mal-jaksel-polisi-selidiki

Detik.com. (2024). 2 Penipu Modus Beli HP Pakai Bukti Transfer Palsu di Makassar Ditangkap. https://www.detik.com/sulsel/makassar/d-7928563/2-penipu-modus-beli-hp-pakai-bukti-transfer-palsu-di-makassar-ditangkap

Detik.com. (2024). Modus Turis Pakistan Bikin Bukti Transfer Fiktif untuk Tipu Restoran di Bali. https://www.detik.com/bali/hukum-dan-kriminal/d-7388220

Republika.co.id. (2024). Kasus Penipuan di Yogyakarta Gunakan Bukti Transfer Fiktif. https://rejogja.republika.co.id/berita/r7utgc327/kasus-penipuan-di-yogyakarta-gunakan-bukti-transfer-fiktif

US DOJ. (2023). Six Defendants Charged in Multimillion-Dollar Check Theft and Bank Fraud Ring. https://www.justice.gov/usao-sdny/pr/six-defendants-charged-multimillion-dollar-check-theft-and-bank-fraud-ring

DigitalTransactions.net. (2023). Concern About Duplicate Checks Rises With Soaring Popularity of Mobile Deposits. https://www.digitaltransactions.net/concern-about-duplicate-checks-rises-with-soaring-popularity-of-mobile-deposits

SPJNews.id. (2025). LSM GMBI Sumenep Soroti Kasus Dugaan Mark-up Invoice yang Dilakukan PLN ULP Ambunten. https://spjnews.id/2025/03/29/lsm-gmbi-sumenep-soroti-kasus-dugaan-mark-up-invoice-yang-dilakukan-pln-ulp-ambunten

Kompas.com. (2023). Kontraktor Mark-Up Harga Pengajuan di Proyek BTS 4G. https://nasional.kompas.com/read/2023/07/04/16224511/kontraktor-mark-up-harga-pengajuan-di-proyek-bts-4g-akibat-fee-10-persen