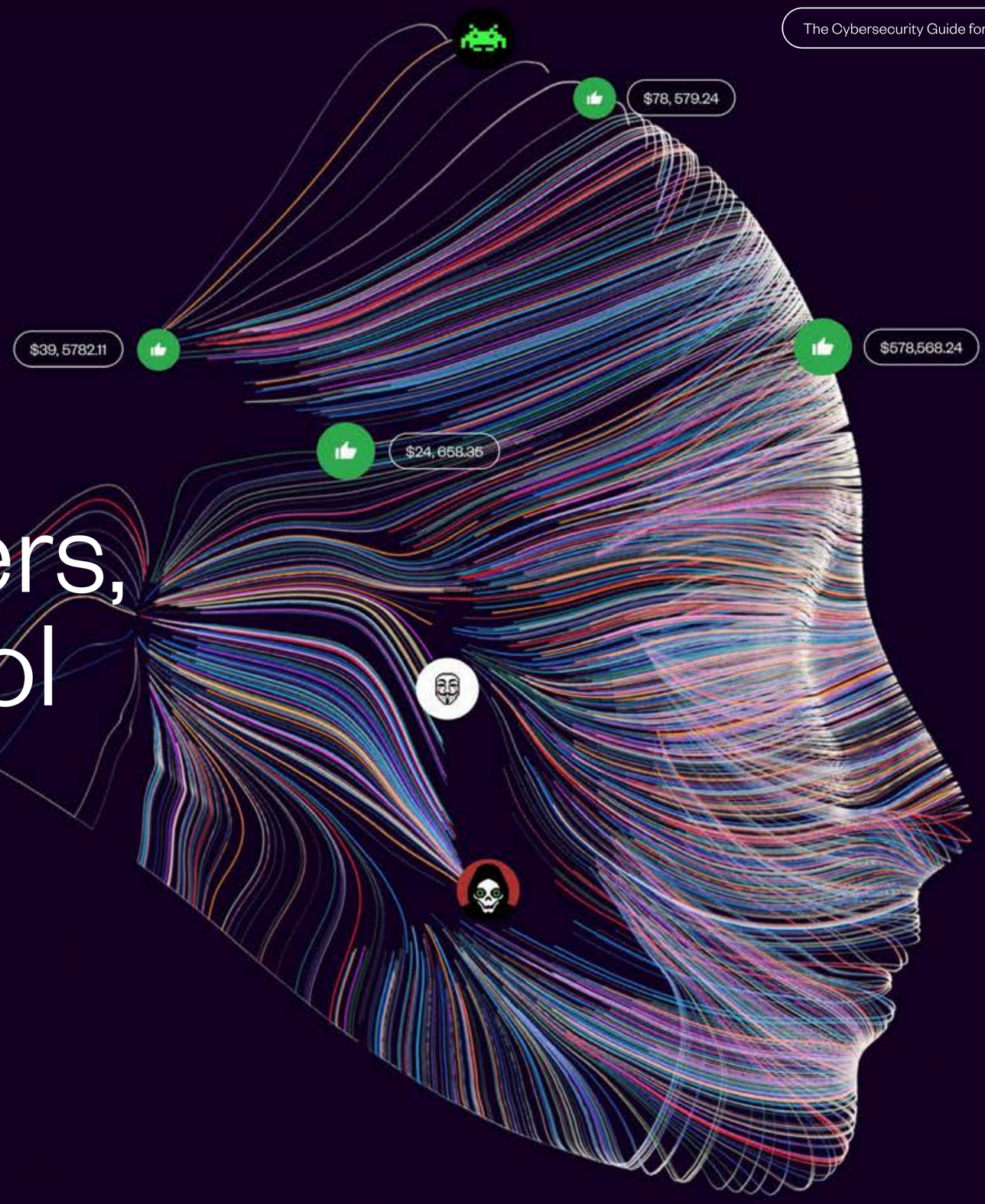


The Cybersecurity Guide for CFOs

Beyond borders, beyond control

Summary

SisID
An eftsure company

SisID
An eftsure company

Editorial

Cybercrime is evolving faster than traditional control measures. The industrialization of fraud, combined with the rise of artificial intelligence (AI), has profoundly altered the risk equation for financial management. Attacks are now inexpensive to deploy, highly targeted, and often conducted from abroad.

In this context, vulnerabilities are no longer just technical. Meticulously organized, payment fraud does not stop at borders or IT perimeters. Internal control measures must therefore evolve at the same pace as international financial flows and the technologies used by fraudsters.

For many European companies, protecting international B2B payments remains a blind spot. ERPs, banking systems, and compliance measures have historically been designed for a domestic framework, while supplier relationships, bank accounts, and payment circuits are now global.

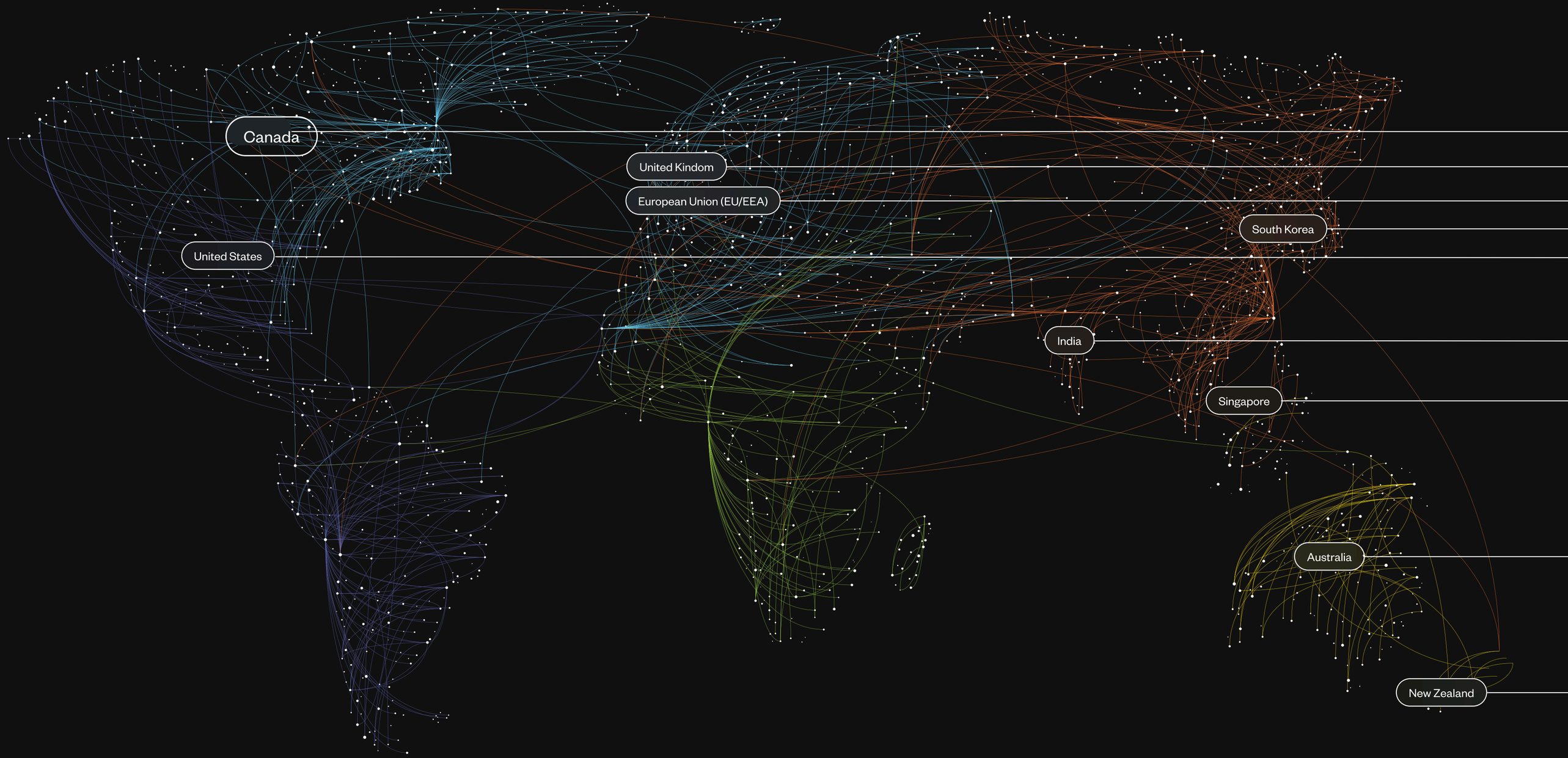
Sis ID (an Eftsure company) was born from this observation. Securing payments can no longer rely solely on manual controls, declarative validations, or trust in entered data. It requires independent, continuous, and operable verification on an international scale.

This guide is aimed at CFOs, Accountants, and Treasurers facing increasing risks of fraud facilitated by AI, heightened regulatory requirements (GDPR, AML-CFT, OFAC...), and increased operational pressure. Securing payments is no longer just an operational issue: it is a matter of governance, compliance, and financial accountability.

Jon Soldan
Chief Executive Officer
Eftsure

SisID
An eftsure company

2026 Risk Map



Region	Regulations / Compliance	Cyber threats	Potential operational errors	Severity for Compliance	Severity of threats	Severity of potential errors
Australia	AML/CTF (AUSTRAC); sanctions (DFAT); privacy (APPs); PayTo/NPPA rules; international reporting on large transfers.	BEC (Business Email Compromise) targeting Australian suppliers; invoice redirection; ATO on online banking; SIM swapping; supplier portal compromise; falsification of QR/PDF invoices.	BSB/account format validation; cut-off times; confusion between NPP and RTGS; remittance data length; public holidays; disclosure of AU$ vs FX conversion.	High	High	Medium
New Zealand	AML/CFT law (DIA/RBNZ/FMA); NZ sanctions; privacy (Privacy Act); international filtering obligations.	BEC via trans-Tasman supply chains; spear-phishing of SMEs; credential stuffing on banks; compromised cloud file sharing for invoices.	Differences in bank/branch format compared to AU; limited availability of instant payments; cut-off times; misalignment of public holidays with AU; transparency of FX fees.	Medium	Medium	Medium
European Union (EU/EEA)	Verification of Payee (VoP) on SEPA transfers; anti-fraud reinforcement via DSP3 / PSR; AML-CTF requirements on third parties.	BEC suppliers; bypassing VoP due to name similarity (shell companies); spoofing (fake bank advisor).	Acceptance of a partial or ambiguous VoP match; over-reliance on a technically valid IBAN; unverified changes to bank details.	High	High	High
United Kingdom	Confirmation of Payee (CoP) on domestic GBP payments; Failure to Prevent Fraud Offence; UK AML/CTF requirements.	Supplier change of details fraud; bypassing CoP through social engineering; mule accounts exploiting instant payments (Faster Payments Service); spoofing (fake bank advisor).	Execution despite non-matching CoP; equating CoP to an anti-fraud guarantee; instant payments executed without post-change review of details.	High	High	Medium
United States	BSA/AML (FinCEN); sanctions (OFAC); ACH Nacha rules; patchwork of state privacy; beneficial ownership reporting; industry-specific controls.	BEC with W9/W8 forms; payroll diversion; supplier portal takeover; check fraud; ATO on small banks; MFA fatigue attacks.	ABA routing errors versus account numbers; ACH timing vs wire; uneven adoption of FedNow/Realtime; cut-off times; addenda limits; intermediary bank fees.	High	High	High
Canada	FINTRAC AML/CTF; sanctions; PIPEDA privacy; EFT/ACSS rules; provincial data residency expectations for certain sectors.	BEC related to US supply chains; falsification of PDF invoices; credential stuffing on banking portals; SMS phishing in English/French.	Formatting of institution/transit/account numbers; choice between EFT and wire transfers; bilingual state references; time zones (NL to BC) and cut-off times.	Medium	Medium	Medium
India	FX controls/remittance reporting RBI; purpose codes; AML/KYC; data localization in certain contexts; GST/tax documentation; UPI rules for domestic flows.	BEC targeting export/import invoices; OTP interception; malicious payment applications; QR fraud; mule networks; SMS/email spoofing.	IFSC/account code formats; mandatory purpose codes; documentation requirements; density of bank holidays; time zone discrepancies; transliteration issues with names.	High	High	High
Singapore	MAS AML/CFT guidelines; sanctions; PDPA privacy; PayNow/Fast rules; cross-border FX documentation for certain transactions.	BEC via regional hubs; SMS spoofing; QR scams; supplier directory poisoning; API credential leaks for MAS-regulated entities.	Choice between FAST and SWIFT; bank/branch code formats; strict narrative field lengths; cut-off times; overlaps of regional public holidays.	High	High	Medium
South Korea	FX remittance approvals/reporting; AML/CFT; PIPA privacy; sanctions; industry-specific export controls in certain sectors.	BEC using Hangul/English code-switching; credential phishing; invoice falsification; social engineering for remittance approvals.	Bank/account code formats; purpose codes and FX documentation; inconsistencies in Hangul/Latin names; cut-off times; local holidays and Hangul/Hanja encoding.	High	High	High

1. The illusion of control

Are current anti-fraud measures sufficient?

SisID
An eftsure company

In many financial departments, payment fraud is perceived as a risk that is already largely covered. Processes are documented, validation circuits are structured, and responsibilities are clearly defined. Sensitive payments undergo enhanced checks, with multiple levels of approval, phone reminders, and local compliance requirements.

These measures are essential. However, they can also create an illusion of control, even as fraud evolves faster than the checks.

Most B2B fraud does not stem from spectacular technical failures, but rather from exploiting vulnerabilities within processes deemed reliable: supplier emails, existing validation circuits, operational urgencies, long-established trust relationships.

Fraudsters are better prepared than ever

Fraudsters today have tools that are equal to or even superior to those of legitimate organizations, without the legal or ethical constraints. They particularly exploit:

- generative AI to produce credible and contextualized messages,
- machine learning to analyze payment cycles,
- automation to operate at scale,
- collecting and exploiting stolen data to personalize each attack,

Example: deepfake videos, voice cloning, synthetic identities, and realistic spoofed domains allow for easy impersonation of executives, suppliers, or even colleagues you interact with daily. Other tools, like the Business Invoice Swapper, amplify existing tactics through the speed and scale offered by AI. These tools, available on the dark web, are often inexpensive, and stolen data is sometimes sold for less than $10.

The role of manual verification in international payments

Manual or semi-automated verification processes remain common, especially for relationships with international suppliers.

This persistence reflects legitimate operational realities:
- fragmented payment systems,
- varying regulations across countries,
- complexity in validating bank details.

However, is this traditional verification approach sufficient to protect financial teams, often limited in staff, constrained by tight budgets and high workloads?

Practical limits of manual controls

They introduce specific vulnerabilities:

- Asynchrony: time zone differences, response delays, operational urgencies,
- Fragmented data sources: ERP, emails, contracts, supplier portals,
- Dependence on individuals: human judgment, local knowledge, continuity in case of absence,
- Risk of error: manual entries, incorrect bank details.

The challenges of verifying international payments

Asynchronous verification

With time zone management, making callbacks can lead to delays of 12 to 24 hours or more, creating windows of vulnerability. During these windows, urgent payment requests are indeed more likely to slip through the established processes.

Heterogeneous data sources

Verifying international banking information often requires cross-referencing data from multiple systems: supplier portals, email threads, contractual documents. This is done without a single source of truth and with limited ability to confirm the authenticity of the data.

Resource constraints

Most organizations perform supplier due diligence only at onboarding, with little ongoing monitoring of their information to detect changes that may signal a compromise or fraud.

Different verification standards

Manual verification processes heavily rely on individual judgment and institutional knowledge. When experienced staff are unavailable, the quality of verification may suffer, particularly for complex international payments where local banking conventions are often less known.

Third-party risk: understanding the new business ecosystem and its hidden threats

Even if internal defenses are strong, your broader ecosystem may not be. Each supplier, partner, and contractor represents a potential entry point – not only into your network but also into your payment flows and financial systems. As supply chains digitize and globalize, the attack surface expands exponentially, as do the opportunities for payment fraud.

Third-party risks: when fraud comes through suppliers

The security of your suppliers directly conditions the security of your payments.

When a supplier is compromised, attackers gain access to:

- Legitimate email exchanges,
- Known payment cycles,
- Usual billing formats,
- Trusted communication channels.

This was the case, for example, with the MGM and Caesars incidents in 2023: both incidents were attributed to the hacker collective Scattered Spider, which infiltrated supplier networks to access the companies' core systems. Once inside the system, attackers used legitimate remote support tools as well as social engineering techniques to elevate their privileges and move laterally within interconnected infrastructures.

The security of your suppliers is your security. And their vulnerabilities become your financial risk.

SisID
An eftsure company

Examples of supplier fraud scenarios:

Invoice manipulation

Attackers often monitor exchanges between accounting teams and suppliers, then inject fraudulent invoices or modify legitimate invoices with falsified banking details. Communication coming from the supplier's actual email system can thus evade traditional checks.

Payment redirection

Fraudsters can compromise a supplier's email or accounting system several weeks or months before the attack. They observe payment cycles and amounts, then send urgent requests to change banking details that appear completely legitimate – often synchronized with actual invoices or known cycles.

Multi-party exploitation

In complex supply chains, a compromised supplier can provide information on multiple downstream partners. Attackers can orchestrate simultaneous fraud across multiple relationships, increasing efficiency and reducing the likelihood of detection.

The blind spot of data sharing in payments

Every international transaction and supplier relationship involves the exchange of sensitive financial information: banking details, transfer instructions, invoices, contacts, and purchase orders. Once this data is out of your direct control, it is only secured by the systems that process it downstream.

For finance departments managing hundreds of European and international suppliers, this creates a cascading risk profile. Each supplier potentially shares payment information with its own providers: accounting firms, payment processors, banking platforms, or software vendors. A breach in this extensive network can expose your business to fraud.

The question is not just: "Can I trust this supplier?" but "What happens to the security of our payments if this supplier is compromised?"

Key points to watch for international suppliers:

Local cybersecurity standards:

Requirements and practices vary by country. Some suppliers may handle your banking information with insufficient protections.

Third-party providers:

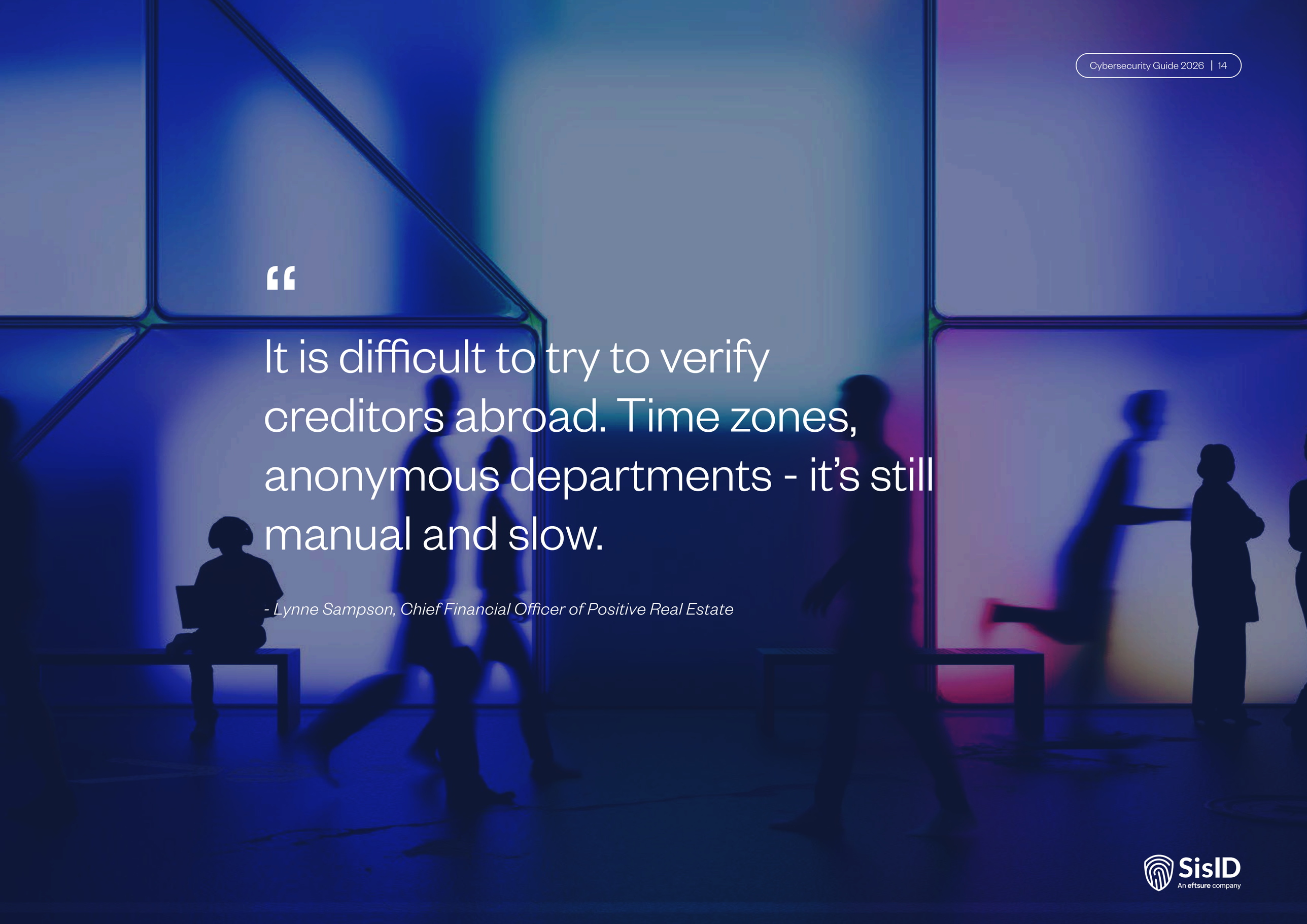
International suppliers often rely on local processors or services that you have never audited, introducing additional vulnerabilities.

Communication security:

Email remains the primary channel for financial exchanges, but many suppliers do not implement security protocols, making forgery easier.

Most companies perform supplier due diligence only during onboarding. Few continuously monitor changes in ownership, compliance, cybersecurity posture, or financial stability.

Result: a network of "trusted" third parties that may no longer be, leaving the door open for fraudsters to exploit payment workflows.



> “
>
> It is difficult to try to verify creditors abroad. Time zones, anonymous departments - it’s still manual and slow.
>
> *- Lynne Sampson, Chief Financial Officer of Positive Real Estate*

SisID
An eftsure company

“

A colleague lost his CFO position due to a fraudulent transaction that came through his email. He sent 175,000 Australian dollars to Singapore... Ensuring that larger transactions arrive at the right place is essential.

- Tyler Casky, Founder and Partner at TheBeanCounters

SisID
An eftsure company

2. The threat landscape

Third-party risks: when fraud involves suppliers

SisID
An eftsure company

Cybercrime is evolving faster than financial teams can adapt with current controls. It is no longer limited to isolated attacks or national targets. Fraud is now international in scope: it integrates into global supply chains, moves through international banking networks, and is perpetrated by large-scale criminal organizations.

33%

$16 BILLION USD

The FBI reported losses of $16 billion related to cybercrime, a 33% increase from the previous year.

SisID
An eftsure company

$6.8 MILLION NZD

61%

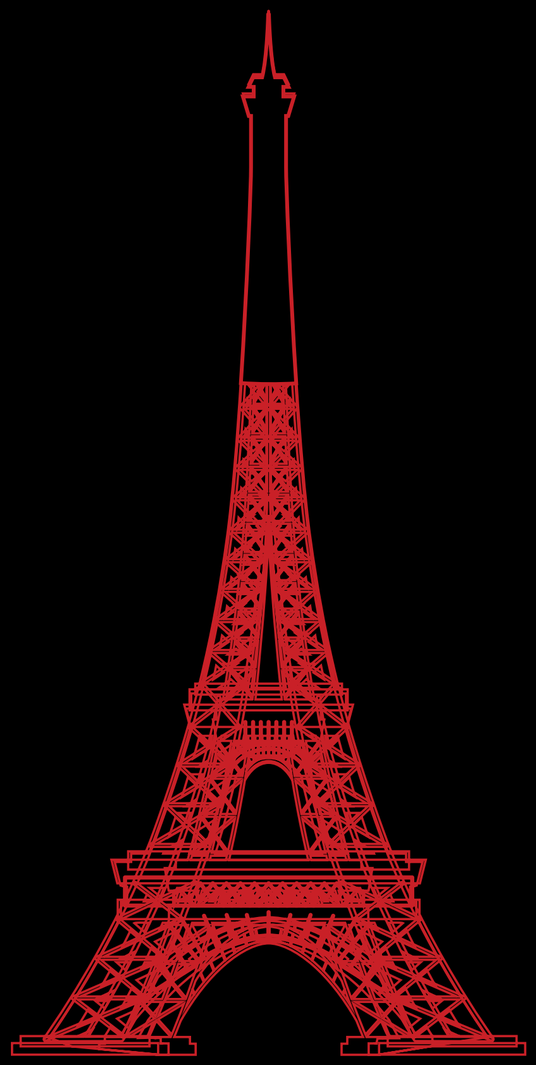
In New Zealand, CERT NZ recorded losses of 6.8 million NZD in the second quarter of 2024, an increase of 61% compared to the previous year.

SisID
An eftsure company

$33,000 AUD/incident

In Australia, nearly half of internet users fell victim to cybercrime in 2024, with average self-reported losses of 33,000 AUD per incident.

SisID
An eftsure company



85% attempts

In France, 85% of mid-sized and small enterprises were targeted by fraud attempts in 2024, up from 60% in 2020. 25% of them fell victim to successful fraud. Memo Bank

SisID
An eftsure company

$10.5 TRILLION USD

Globally, losses due to cybercrime are expected to reach $10.5 billion annually by the end of 2025.

SisID
An eftsure company

"As soon as there is human interaction, particularly when there is a single point of failure or one person in charge of the case, it becomes relatively easy to modify a bank account. This opens the door to fraud."

- Tyler Casky, Founder and Partner at TheBeanCounters

Evolution of B2B Tactics and Social Engineering

BEC (Business Email Compromise) groups are now using data from security breaches, spoofed domains, and commercially available AI tools, such as:

- ElevenLabs, which allows for voice cloning to impersonate real people
- Synthesia, used to create realistic deepfakes
- WormGPT, a dark web tool designed to help criminals write convincing fraudulent emails and identify vulnerabilities
- ScamAgent, a fully automated agent combining multiple AI capabilities to attack businesses in a nearly autonomous mode

Data breaches also provide access to real emails, payment histories, and contact chains. This allows fraudsters to increasingly replicate perfectly legitimate supplier interactions.

However, it is important to remember that a large part of B2B fraud does not require a major or highly publicized breach. It can also stem from routine payment processes lacking verification, starting with seemingly minor elements: a modified bank account number, a spoofed contact, or a missed phone call. These attacks are common, do not rely on major systemic failures, but simply exploit gaps in trusted workflows.

The Economy of "Scam Compounds"

In some Southeast Asian regions, cyber fraud has become a structured industry. "Scam compounds," or "slave farms," located in Cambodia, Laos, and Myanmar are said to have forced thousands of human trafficking victims to work full-time in online fraud. These structures target foreign businesses through fake supplier profiles, investment scams, and identity theft techniques.

Although some government actions have been taken against these centers, there is little evidence of their effectiveness or their inclusion in a sustainable strategy to combat organized crime. Investigations, including by the Guardian, even show that some of the most well-known complexes have expanded in size and number.

Furthermore, Interpol's First Light operation (2023) led to 3,400 arrests and the seizure of over 300 million USD in 61 countries. In 2024, the operation resulted in the arrest of 3,950 suspects and the identification of 14,643 potential suspects across all continents. These figures clearly show that these frauds are neither isolated nor local: they operate on a global scale and rely on international banking systems.

3400 arrests and the seizure of more than

$300 BILLION USD

in 61 countries

Source: Australian Strategic Policy Institute via Google Earth

3,950

Suspects in the Philippines

14,643

Suspects across all continents

The First Light 2024 operation led to the arrest of 3,950 suspects, as seen here in the Philippines, and identified 14,643 other potential suspects across all continents. Source: Interpol.int

The data contained in portable devices, computers, and phones seized during the First Light Operation, such as these in Hong Kong, have been sent to the INTERPOL General Secretariat for analysis. Source: Interpol.int

When B2B Payments Fund Organized Crime

In 2024, a global operation called Operation TENTACLE revealed and exposed criminal networks using legitimate B2B channels to launder funds internationally. Following these revelations, the World Customs Organization called for policy reforms to address vulnerabilities in international payments.

This is not just a financial issue. Payments made to unverifiable suppliers expose businesses to significant regulatory, reputational, and operational risks. These transactions are often processed perfectly legally and are only reported once the harm has been done.

Thus, B2B payment fraud goes far beyond the issue of financial loss: it is one of the mechanisms for funding organized crime. Unverified payments made in good faith can feed accounts controlled by criminal networks, financing broader illicit activities: scam compounds, human trafficking networks, and international money laundering circuits. These networks are not marginal; they are an integral part of the global cybercrime infrastructure.

3. The challenges of International Compliance

Cybercrime is international – and industrialized

SisID
An eftsure company

No jurisdiction approaches payment compliance in the same way. From supplier onboarding to payment controls, reporting, and traceability, finance departments operating internationally must navigate a fragmented set of overlapping and rapidly evolving regulations.

The work of European and international authorities shows significant inconsistencies in the supervision of payment service providers, particularly regarding anti-money laundering, beneficiary verification, and reporting obligations, especially for international flows.

For Finance Departments, this fragmentation complicates internal control: a compliant payment in one country may expose the company to regulatory risk in another.

Financial sanctions: a multiple and evolving framework

European companies must comply with several sanction regimes:

- EU sanctions lists,
- national sanctions (for example, from French, German, or Italian authorities),
- international sanctions that de facto apply to euro or dollar flows.

These lists frequently evolve, and compliance is a legal obligation, even in cases of unintentional violation. Consequences can include significant fines, asset freezes, activity restrictions, and lasting damage to the company's reputation.

In an international context, complexity increases: a supplier authorized in one jurisdiction may face restrictions in another. The responsibility of the ordering party remains engaged, even when fraud is 'suffered'.

A patchwork of data protection rules

Data protection regulations add an additional layer of complexity. In Europe, the GDPR strictly governs the storage, processing, and sharing of certain business data, including data related to suppliers and payment beneficiaries.

Teams must comply during audits, and complexity increases particularly when control tools or partners are located outside the European Union. When the identity of the beneficiary or bank details cannot be validated through independent sources, the risk of error or fraud mechanically increases.

At the same time, regulators are tightening transparency requirements. Developments related to ISO 20022, beneficiary verification (VoP) for SEPA payments, or AML-CTF obligations require profound adjustments to systems and processes, often on still heterogeneous infrastructures.

> The solution is not to have more documentation. It is rather to build processes that people understand and follow because they work, not simply because they are required.

Why compliance can no longer be just a simple 'tick box'?

In the face of this complexity, many organizations respond by adding controls: additional validations, email exchanges, phone reminders, increased documentation. This approach may create an illusion of compliance, but it undermines operations.

Manual controls slow down payment cycles, increase the risk of error under pressure, and do not meet the demands of an environment of industrialized fraud.

The acceleration of payments: an additional risk factor

European initiatives to accelerate international payments – SEPA Instant, modernization of infrastructures – mechanically reduce control times.

If verification mechanisms are not integrated upstream of the payment, as required by the new VoP regulation, exposure to risk increases. International finance will be faster, but it must first be safer.

Effective compliance does not rely on more documentation, but on integrated, understandable, and genuinely operable processes by finance teams.

4. Sectoral mechanisms and current limitations

What regional frameworks offer and the remaining gaps

Around the world, governments and industry bodies are implementing mechanisms to combat fraud, recover funds, and restore trust in digital payments. These efforts are making real progress, particularly for domestic transactions. However, for international payments, coverage remains limited, inconsistent, or even completely unavailable.

In the United States, the Nacha model includes recommended rules for recovering misdirected funds and establishing clear expectations for data accuracy. The initiative has led to enhanced integration of providers and increasing cooperation among financial institutions.

In Australia and New Zealand, the current rollout of Confirmation of Payee (CoP) demonstrates the potential for coordinated action. CoP protects domestic bank payments by confirming that the account name matches the intended recipient, a simple check that prevents common redirect fraud.

At the European Union level, the Verification of Payee (VoP) regulation requires similar protections for SEPA transfers. Globally, data-sharing efforts in the industry are multiplying, including vendor filtering platforms and early warning systems.

The table on the following page compares the main regional frameworks. It shows what exists, who is protected, and what gaps remain for international transactions.

Region	Verification and refund mechanisms	Existing databases	Information sharing	Regulatory framework
USA	The Nacha regulation provides limited recovery for authorized payments (mainly through ACH networks).	Lack of a national database, each institution relies on its own system.	Nacha has created working groups, FS-ISAC, interbank alerts.	AML/CFT supervision by FinCEN, initial advances towards a refund policy based on standards developed by the private sector.
EU	Verification of Payee (VoP) protects against payment errors but does not systematically guarantee a refund.	VoP is an initiative in the EU aimed at harmonizing payment data. Each PSP can decide on the level of sensitivity for matching.	European Payment Council (EPC) and European Banking Authority (EBA).	Revision of the Payment Services Directive (PSD3), the Instant Payment Regulation (IPR), and European plans for coordination against international fraud.
AUS - NZ	No refunds are mandatory, some are made by banks as a goodwill gesture.	ACCC Scamwatch, ASIC alerts but lack of sharing with banks.	ABA forums, Reporting Scamwatch, AUSTRAC-led collaboration.	Anti-Fraud Centre, ePayments Code, AML/CTF Legislation.
Global/Industry	Voluntary protection mechanisms based on VoP tools and vendor validation solutions.	A few private actors.	FS-ISAC, SWIFT fraud group, banking partners.	G20 roadmap on international payments, FATF travel rule, and guidelines for migration to ISO 20022.

European and national initiatives.

In Europe, Verification of Payee (VoP) represents a significant advancement for SEPA transfers. By comparing the beneficiary's name with the entered banking details, it helps prevent certain payment redirect frauds. However, this mechanism does not guarantee protection for non-SEPA payments.

At the national level, several member states have established reporting and prevention mechanisms, often led by financial or banking authorities. VoP has helped harmonize these initiatives at the regional level.

Information sharing and interbank cooperation.

Market initiatives also exist regarding information sharing and fraud intelligence, notably through:

- sectoral working groups, interbank forums, mechanisms coordinated by central banks or supervisory authorities.

These mechanisms improve the detection of known fraud patterns but still rely heavily on post-incident exchanges and national boundaries. They do not allow for systematic and real-time verification of international payment beneficiaries.

Three immediate actions to reduce your exposure risks.

• Identify your international payments and the associated controls.

• Integrate verification at every stage of the payment process, not just at the onboarding stage.

• Monitor changes in regulations, refund policies, and fraud techniques across all regions where you operate.

While governments and professional bodies strengthen protection systems, CFOs can take steps now to prevent high-risk payments from turning into major financial losses.

SisID
An eftsure company

“

Manual checks work if you are in the same office. Once your business is multi-site, multi-currency, multi-country, technology becomes essential.

- Tyler Casky, Founder and Partner at TheBeanCounters

SisID
An eftsure company

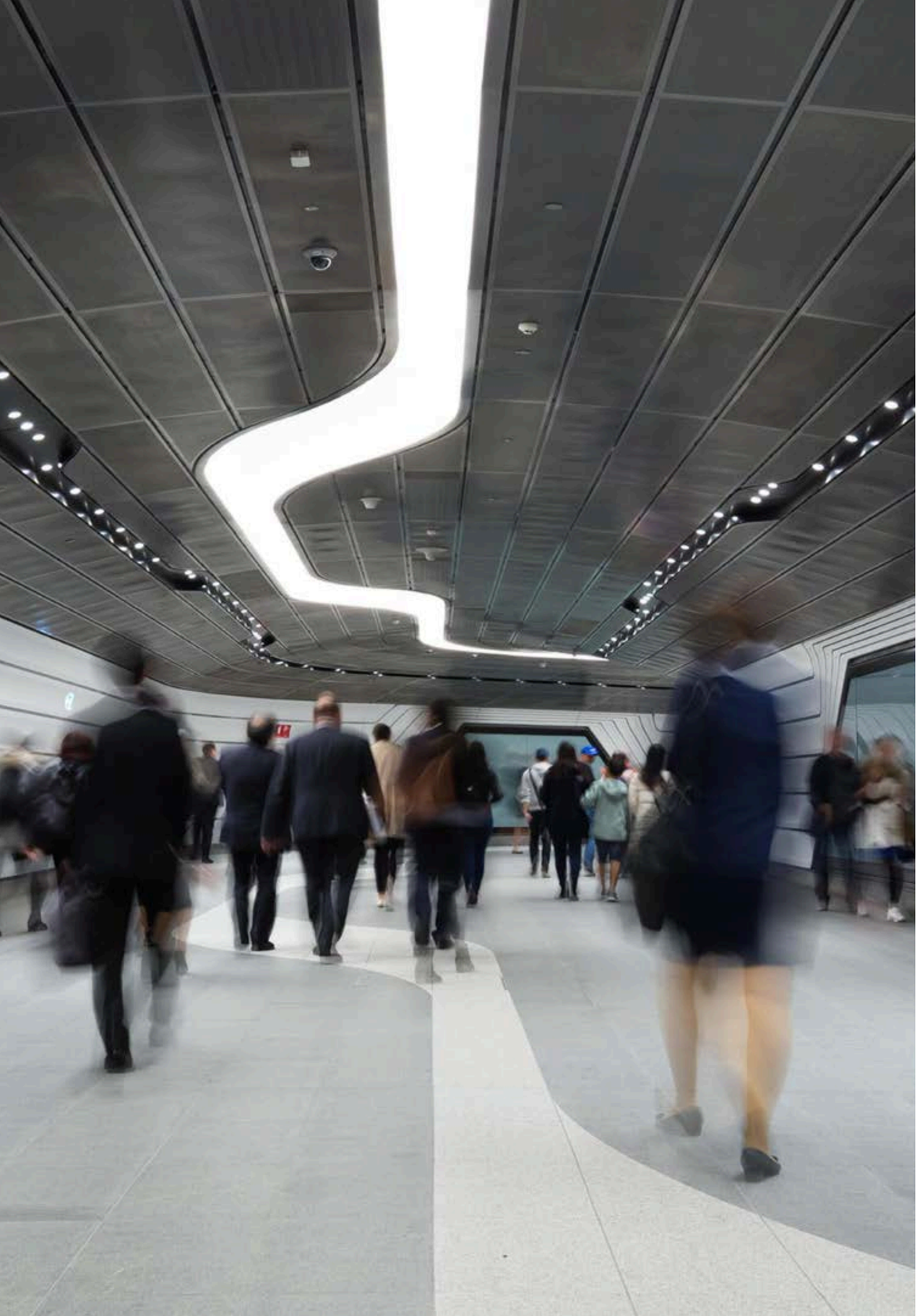
5. Ensure lasting security international payments

Transitioning from a one-off check to a structured and governed system

SisID
An eftsure company

> “The reality is before us: the actors trying to harm us excel at what they do. We must be better. And this is where the CFO has a role to play.

- Kevin O’Sullivan, Chief Financial Officer at CyberCX (via October 2025 webinar)



In the face of the industrialisation of fraud and the acceleration of payments, traditional measures are reaching their limits. Ensuring the security of international payments cannot rely solely on a buildup of manual controls or the vigilance of teams.

It is about integrating verification into the core of the internal control system, with a structured, measurable approach that complies with European regulatory requirements.

Financial leaders face a dual challenge:

1. Protecting their organisations against increasingly convincing fraud attempts

2. Maintaining the speed and efficiency essential to business realities

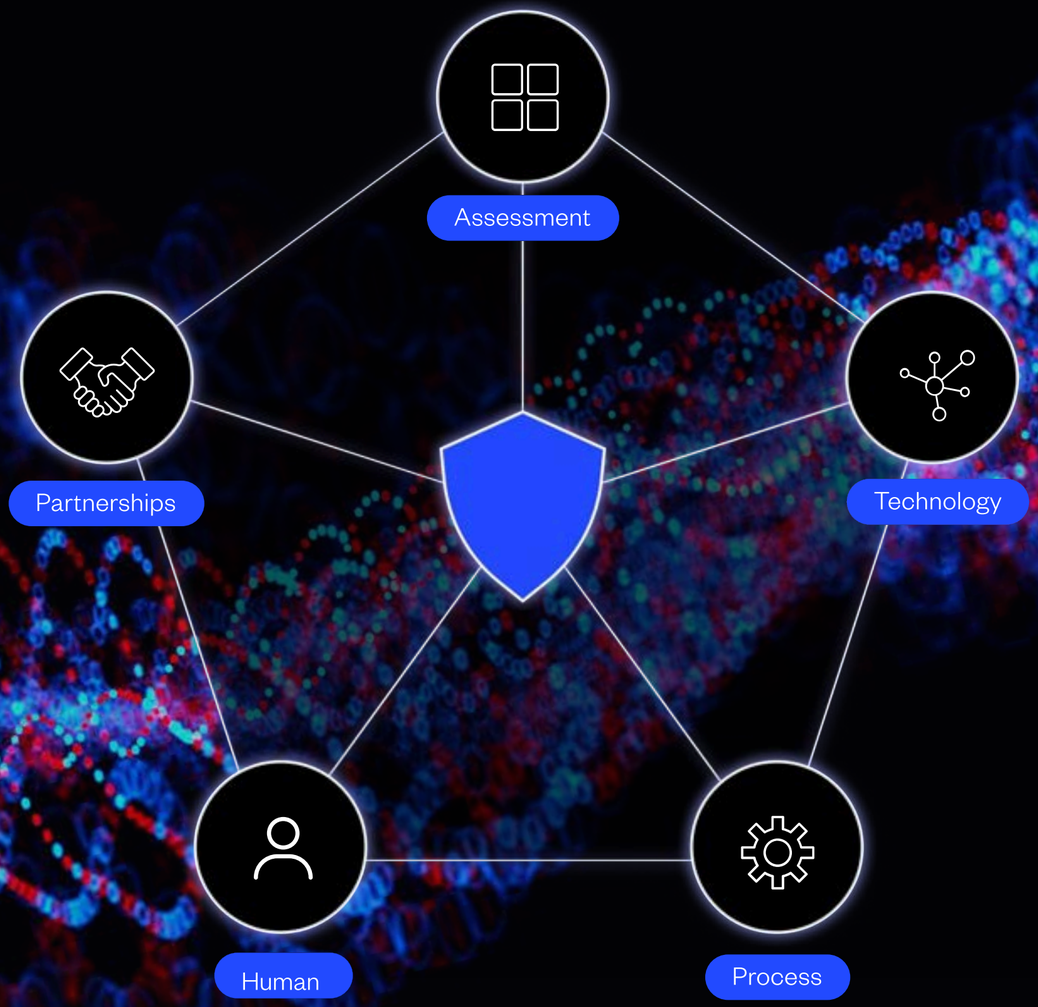
This dual challenge is particularly difficult when it comes to international suppliers, where language barriers, time zone differences, and unfamiliar banking systems create additional vulnerabilities that fraudsters actively exploit.

The good news is that strengthening payment controls does not mean sacrificing efficiency. Often, a systematic approach to fraud prevention will also streamline legitimate transactions, reduce processing times, and improve relationships with suppliers.

SisID
An eftsure company

A five-pillar control framework

The most mature organisations rely on a framework based on five complementary pillars.



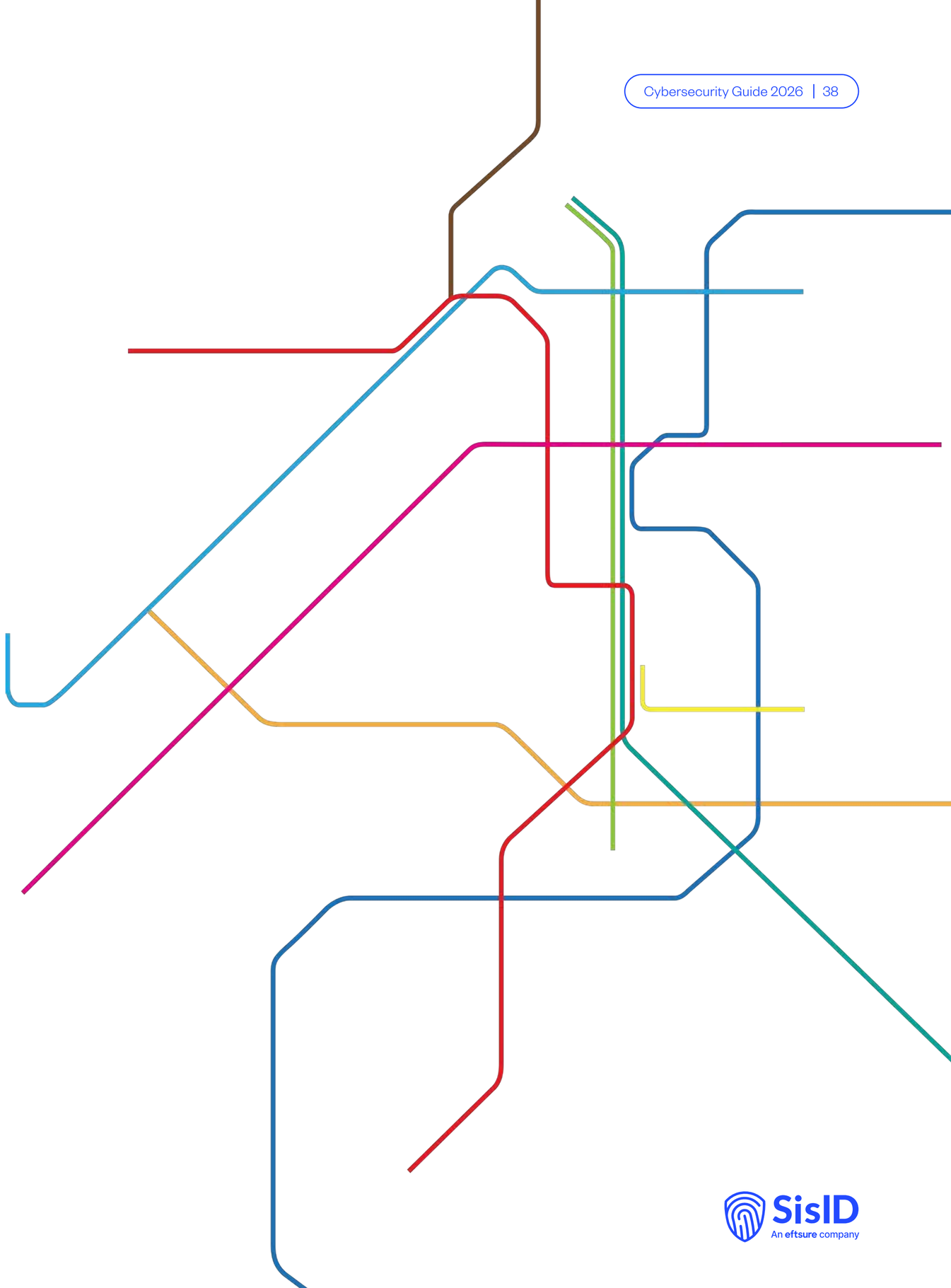
Assessment:

Mapping payment-related risks

The first step is to accurately identify the exposure areas:

- recurring international payments,
- critical or strategic suppliers,
- high-risk countries (fraud, sanctions, regulatory instability),
- sensitive scenarios (change of bank details, urgent payments, exceptions).

This mapping allows financial departments to prioritize controls and allocate resources proportionately to the risk.



SisID
An eftsure company

Technology:

Integrate an independent and automated verification:

Supplier detail verification can no longer rely solely on data entered in the ERP or sent via email.

An effective system relies on:

- an independent data source,
- automated verification,
- direct integration with ERPs and accounting tools.

This approach reduces the risk of human error, enhances traceability, and allows for international operations without burdening processes.

SisID
An eftsure company

“

Restricting social engineering by implementing a control system is the best solution. A gateway like Eftsure, for example, makes things too difficult for me as a hacker.
I would then move on to the next easy target, as it is guaranteed that there won't be many organizations doing what I just suggested.

- Bastien Treptel, cybersecurity consultant and former hacker (via On The Defense, Sydney)

Processes

Formalize and secure sensitive workflows

The most exposed processes must be subject to clear and documented rules, particularly for:

- changes to supplier bank details,
- urget or exceptional payments,
- derogations from standard circuits.

The goal is not to multiply validations, but to ensure consistency, traceability, and auditability of decisions, within an internal control and compliance framework.

SisID
An eftsure company

Human

Training and empowering finance teams

Even the most advanced technological systems remain ineffective if teams are not trained and aware.

Financial departments must invest in:

- training on new fraud schemes,
- the understanding of AI usage by fraudsters,
- the identification of weak signals.

Giving employees the legitimacy to question a payment, even if formally approved, is a key prevention lever.

Ecosystem

Relying on partners capable of operating at an international scale

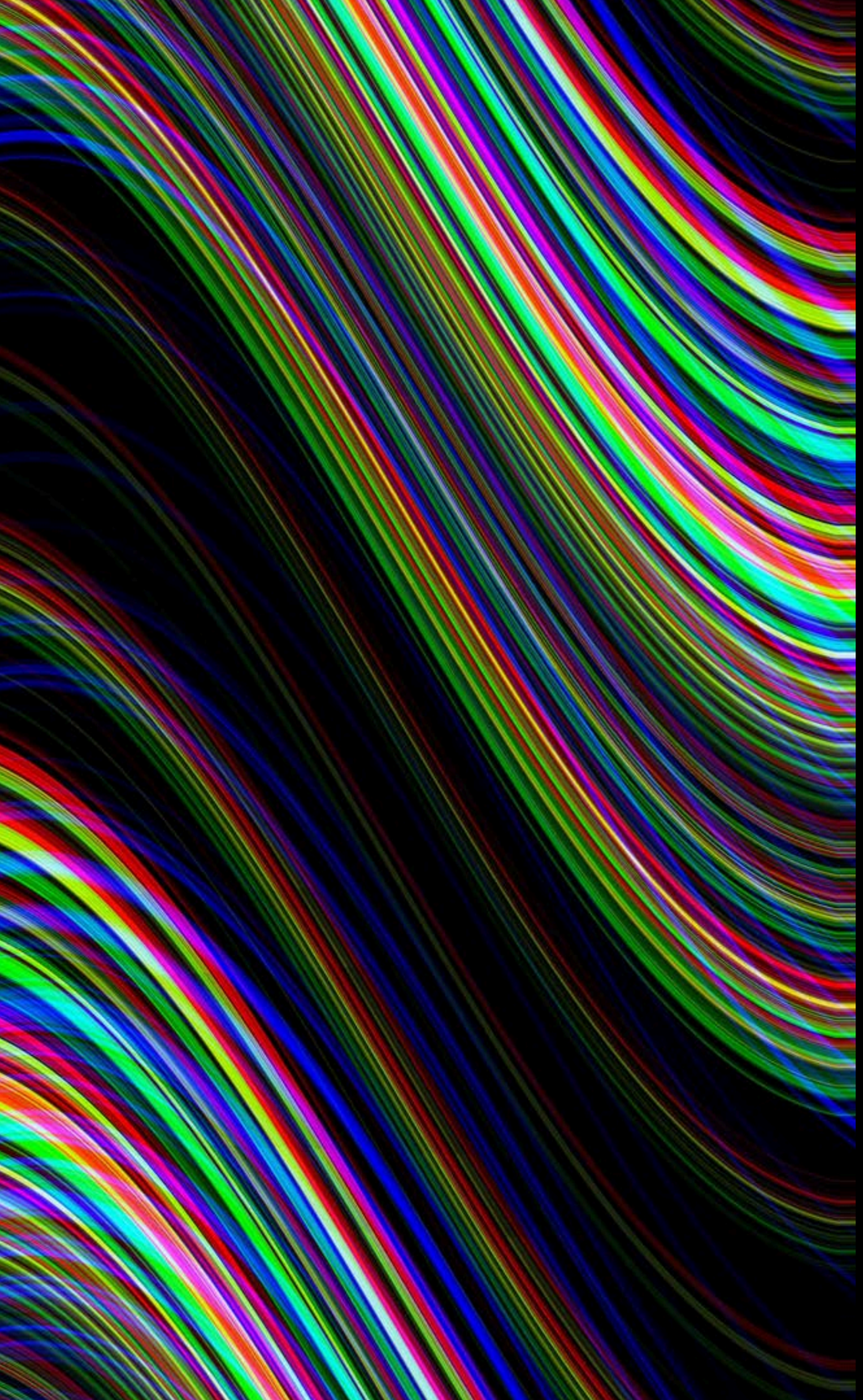
No organization can, on its own, maintain a comprehensive view of global fraud risks.

Relying on specialized partners allows for:

- pooling risk signals,
- benefiting from continuous monitoring,
- operating across multiple jurisdictions with consistent standards.

For CFOs, this choice is a governance decision, just like choosing an ERP or a banking institution.

SisID
An eftsure company



Resources to level the playing field against AI-driven fraud

Assessment of vulnerability to deepfakes

Anti-Cybercrime Strategy Guide

Standard responses that help staff combat fraud

SisID
An eftsure company

6. Conclusion

Why 2026 is a pivotal year

B2B payment fraud is no longer a marginal or operational risk. It now sits at the intersection of:

- financial risk,
- regulatory risk,
- reputational risk.

Whether your company has already been a victim of attempted fraud or not, you can take control starting today. The five-point framework provides a clear path forward. It is not a question of the legitimacy of financial teams to lead a strategy against cybercrime — it is their responsibility.

The upcoming enforcement of DSP3, the widespread implementation of Beneficiary Verification, the acceleration of instant payments, and the massive use of AI by fraudsters are fundamentally changing the risk equation.

For financial management, 2026 marks a turning point: failing to integrate international payment verification into the control process exposes the company to direct losses, as well as compliance failures and liability issues.

Regaining control of international payments does not mean slowing down operations, but rather securing growth in an increasingly demanding regulatory and operational environment.

SisID
An eftsure company

About Sis ID

SisID
An eftsure company

What if you no longer had to worry about fraud?

Sis ID is a French fintech founded in 2016 by CFOs and Treasurers from the CAC40. It assists companies in detecting and preventing financial fraud, both in France and internationally.

Our solution allows you to:

- Secure your payments by verifying the bank details of your partners,
- Anticipate fraud attempts,
- Keep your supplier database up to date,
- Streamline processes from purchase to payment.

Since 2025, Sis ID has joined Eftsure, a leading player in payment security for over 10 years. Together, we are becoming the world's leading player in securing payment flows with international coverage and impact.

With Sis ID an Eftsure company, let’s facilitate payment security on a global scale.

SisID
An eftsure company

Without Sis ID

Step 1 — Step 2 — Step 3 — Step 4

Integration of new suppliers & Management of supplier changes

In organizations without a secure onboarding process or change request, fraudsters can intercept and alter supplier details.

Change requests could be accepted via email or with a callback check where there is a high vulnerability to fraud and cybercrime such as social engineering.

Fraudsters often monitor email threads before sending targeted "updated bank details."

Risk created:

Teams may inadvertently store fraudulent or manipulated bank details in the Supplier File or ERP. Once incorrect data is in the system, every future payment is at risk.

Supplier base cleaning

Without regular cleaning and updating, a Supplier File quickly becomes inaccurate.

Supplier information is added manually, often copied from websites or emails without anomaly detection, so inconsistencies or anomalies can go unnoticed.

Risk created:

A fraudster only needs a single entry point to intercept or manipulate future payments.

Payment file review

A member of the accounting team prepares payment processing in the ERP, unaware that the supplier's bank information has been compromised.

International payments are already more difficult to validate, with foreign banking formats, time zones, and language barriers, and AP teams rarely have 100% certainty.

The finance team assumes the recorded supplier details are correct, approves the payment, and transfers funds.

Once funds are transferred internationally, it is nearly impossible to recover them.

Risk created:

Fraudulent bank information can silently infiltrate the payment file, without alert or red flag.

If there is no segregation of duties, the same staff member may enter the data but also approve it, increasing the risk of internal fraud.

Discovery

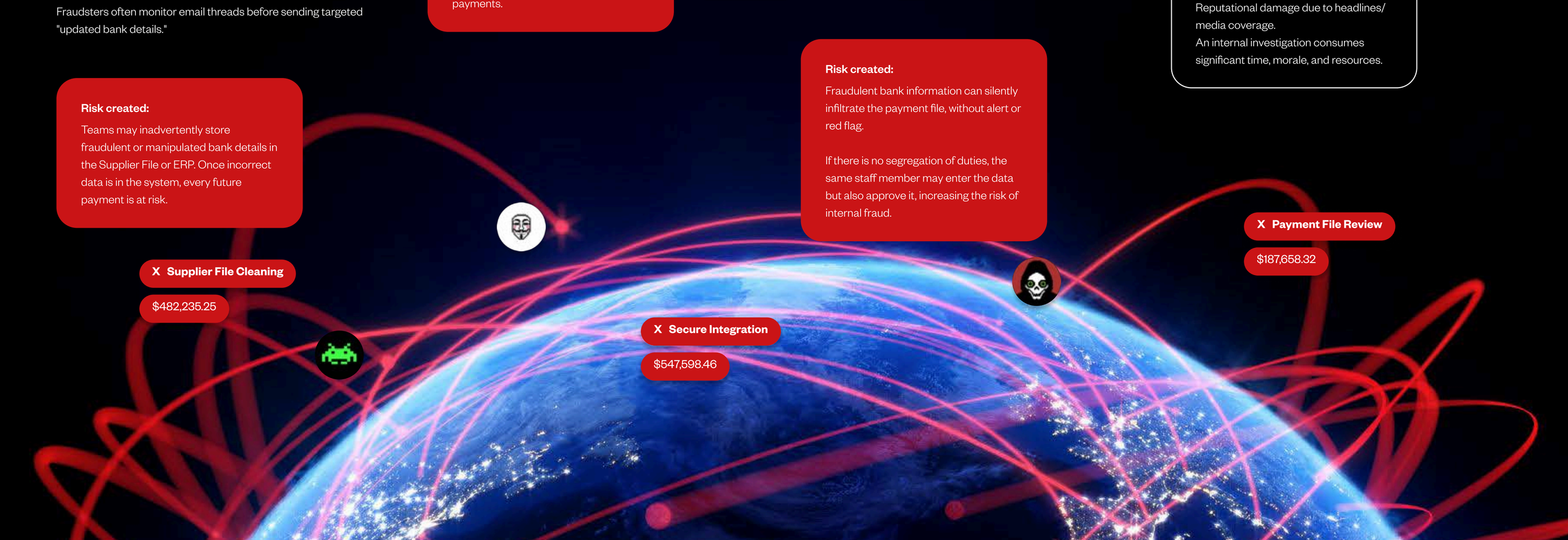
The legitimate supplier follows up on unpaid invoices.

The internal audit notices an unusual update to the supplier. By then, the funds have already been transferred.

Outcome:

Financial losses often range from tens of thousands to millions of dollars.

Supplier relationships become strained. Reputational damage due to headlines/ media coverage.
An internal investigation consumes significant time, morale, and resources.



With Sis ID

Step 1 — Step 2 — Step 3

Integration of new suppliers

Supplier payment data is verified at the time of record creation. Even from unsecured sources, such as emails, it is automatically checked by Sis ID.

The results are immediately interpretable through a simple colour code:
green for reliable information,
red for risky information,
orange for cases requiring further investigation.

Sis ID offers manual accreditation of bank details, conducted by teams of experts trained in detecting complex fraud, thus limiting manual operations and risks for your teams.

Supplier base update

Sis ID allows for regular auditing of existing payment data.

Incorrect, outdated, or fraudulent information is quickly identified, enhancing the reliability of business references.

Similarly, any change in a supplier's bank details is directly secured, reducing the risk of fraud through subsequent payment diversion.

Payment preparation

During payment campaigns, Sis ID effectively manages fraud and payment rejection risks.

Teams no longer have to perform lengthy and fallible manual checks. They can validate payments with confidence, thanks to financial coverage of up to $1M in case of fraud, applicable to supplier/bank details combinations validated by Sis ID.

Each check also generates an audit trail, simplifying the documentation of operations for internal and external audits.

SisID

An **eftsure** company

Technology gives an advantage to cybercriminals.
Sis ID restores the balance in your favour.