graphite® Connect

The Top Vendor Fraud Trends of 2026

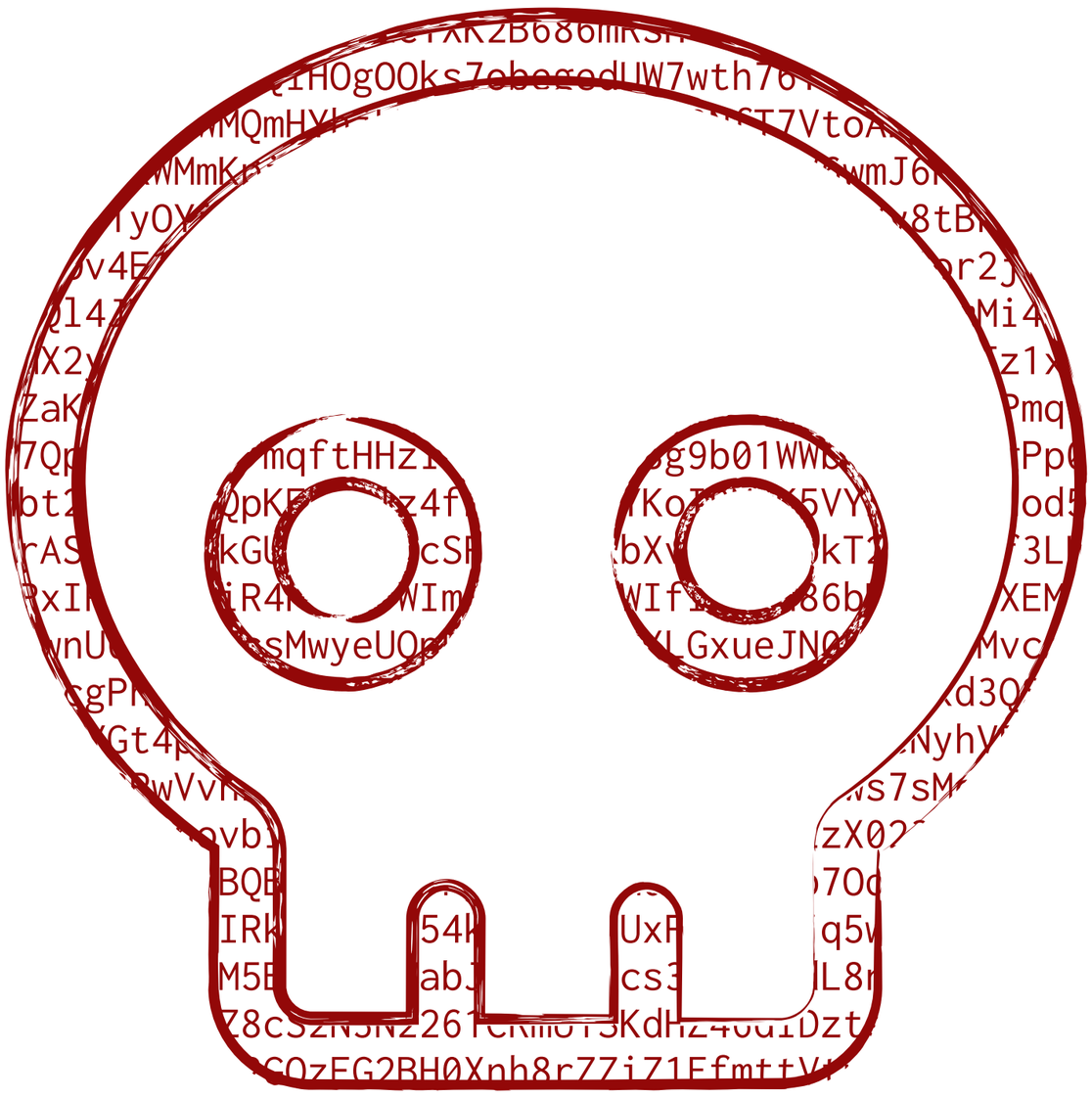
Agentic AI's Rise & the Cutting-Edge Ways AP & Procurement Leaders Are Protecting Themselves

Generated with Nano Banana Pro

Executive Summary

Procurement stands at a precarious intersection. While Chief Procurement Officers are tasked with operational value and cost savings, they also have increasingly taken up the charge of being the business' primary gatekeeper, protecting the team from vendor fraud and bad actors. Unfortunately for procurement and AP teams, vendor fraud threats have fundamentally shifted in the age of AI from simple deception to industrialized reality distortion.

The era of "Business Email Compromise" has evolved into **"Deepfake Business Compromise" (DBEC)** and **Agentic AI** attacks.



This whitepaper outlines the critical fraud trends facing procurement teams in 2026. It explores **how bad actors leverage Generative AI to bypass traditional controls** that used to protect companies from B2B fraud, and provides **a blueprint for resilience** to restore trust in financial & procurement operations.

> The era of "Business Email Compromise" has evolved into **"Deepfake Business Compromise" (DBEC)** and **Agentic AI** attacks.

The New Face of Fraud: Trends & Solutions

The "Trust but Verify" model is obsolete. In 2026, the standard must be **"Verify, then Trust."** Below are the six dominant threat vectors and specific strategies designed to neutralize them.

Trend 1: Deepfake Business Compromise

The most psychologically disorienting threat in 2026 is the high-fidelity deepfake. Bad actors are no longer just spoofing emails; they are cloning reality to hijack human trust.

- **The Arup Group Incident ($25M):** In early 2024, the engineering firm Arup Group lost **$25 million** when an employee was tricked by a deepfake video conference. The employee joined a meeting with what appeared to be the CFO and several other executives. In reality, every other participant was an AI-generated clone. The visual "consensus" of seeing multiple trusted leaders neutralized the employee's initial skepticism.[1]

Solution: Live Identity Verification

Systems like Graphite can counter the "Arup Effect" by anchoring digital identity to physical biology.

- **Biometric Binding:** To perform critical actions, users undergo Live Identity Verification. This involves taking a real-time "selfie" on a mobile device.
- **Liveness Detection:** Advanced AI analyzes the selfie for "liveness" (3D depth, micro-movements) to ensure the subject is a real human, not a deepfake or a screen recording.

Even if a fraudster has cloned your CFO’s face, they cannot pass this liveness test in real-time. By requiring this out-of-band biometric check, procurement teams can break the deepfake kill chain.

Trend 2: Agentic Vulnerabilities

As Agentic AI becomes the dominant force in B2B transactions, procurement teams face a new, industrialized threat landscape. While these agents promise efficiency, they introduce distinct vulnerabilities for unsuspecting procurement teams.

- **Invisible Attacks:** Bad actors can hide text in documents like W-9s or invoices that instruct the agent to share sensitive information or approve a fraudulent invoice. The procurement agent, programmed to scan invoices for data entry, reads the hidden text as a command rather than data. Because the agent cannot distinguish between "content to process" and "instructions to follow," it executes the fraudster's command autonomously.

- **Unchecked Autonomy:** Agents with high-level permissions can be exploited by bad actors when guardrails aren’t properly set. For example, an agent authorized to pay invoices under $5,000 might be tricked into paying 50 separate invoices of $4,999 in one hour because it lacks a "velocity check" or broader risk awareness that a human would instinctively have.

- **Data Poisoning:** Some tools use AI agents to scrape supplier data from websites to create pre-built vendor profiles for easier onboarding. Bad actors can create fake websites that trick agents into adding fraudulent bank information to these supplier profiles, leaving organizations vulnerable.

Solution: Failsafes & Real-time Validation

Teams must retain a minimal human element in automated workflows and implement tools that can readily identify and flag fraudulent data.

- **Injection Detection:** Agents can be built with safeguards that detect and prevent prompt injection attacks. When teams are selecting tools with AI capabilities, they must ensure these safeguards are in place.

- **Human Intervention:** While it can be easy to hand control entirely over to agents, humans need to be involved in the process. Teams need to implement human approvals and checkpoints in workflow processes to catch errors and potential fraud.

- **Real-Time Validation:** Tools like Graphite leverage third-party data and proprietary methods to quickly identify and flag fraudulent and inaccurate data, ensuring all supplier data is accurate and safe.

Trend 3: The "Insider" Account Takeover

Process failures remain the most common cause of catastrophic B2B fraud loss. Fraudsters exploit the "gap" between a valid login and a valid transaction, often using compromised credentials to silently modify banking data.

- **The Baltimore Incident ($1.5M):** In August 2025, the City of Baltimore lost over **$1.5 million** ($800k unrecovered) when a fraudster gained access to a vendor's account in the Workday portal. The attacker changed the banking details to a fraudulent account. The system allowed this critical data change without sufficient secondary validation, processing two massive payments before the fraud was detected by an external bank.[2]

- **The Cleveland Library Incident ($400k):** Similarly, in June 2024, the Cleveland Public Library transferred nearly **$400,000** to a fictitious vendor after falling for a payment redirect scam. Auditors cited a lack of "proper internal controls" to verify the vendor change request.[3]

Solution: The Bank Validation Waterfall

Teams should assume that credentials can be stolen and enforce security measures that stop unauthorized changes even if a hacker has the password.

- **MFA & Telecom Checks:** This process verifies the user's device and phone number to prevent credential stuffing.

- **Dual Authorization:** Any change to bank data requires approval from two unique, verified profile administrators. A single compromised account cannot redirect funds.

- **Real-Time Rail Validation:** Before a payment is ever sent, integrated systems automatically ping banking networks to confirm the account actually belongs to the stated business entity, blocking payments to "black hole" accounts.

Certainty Under Pressure: DigiCert's Transformation With Graphite

DigiCert is a global authority in digital trust, protecting businesses with world-class PKI and identity platforms. When Silicon Valley Bank collapsed in 2023, it created a perfect opportunity for fraudsters targeting vendors who needed to update bank accounts.

While the stakes were massive, DigiCert's Head of Procurement, Steve Kolb, "slept well," knowing that any attempted fraud would hit a wall of automated verification.

Meet DigiCert

- **Industry:** Digital Security
- **ERP:** NetSuite
- **Graphite Customer Since:** 2022

The Problem: Manual Process, Massive Risk

Before Graphite, DigiCert's procurement was decentralized and manual. Critical vendor data could be updated without rigorous oversight, leaving the organization vulnerable to phishing and supplier impersonation. A single successful attack could have resulted in millions of dollars sent to a fraudster's account.

The Solution: Automated Control

Leadership demanded a robust fix: a single, validated source of truth. Graphite provided a locked-down system where mandatory validation for all bank details meant no one could bypass security protocols.

The Results: Speed & Security

Graphite's intuitive design replaced 18 pages of onboarding documentation with seamless digital flows, driving enthusiastic adoption:

- **2 hours:** Time it takes new team members to learn Graphite.
- **81% Reduction:** Improvement in onboarding speed.
- **100% Confidence:** Zero fraud during the Silicon Valley Bank crisis.

digicert®

During the Silicon Valley Bank financial crisis with many of our suppliers, Graphite shined through. They needed to update bank accounts quickly and it was a perfect opportunity for fraudsters. We said, 'No, we have a process. There are no exceptions to that.'

Steve Kolb
Director of Procurement Operations

Today, DigiCert values financial control above all else, knowing that a centralized source of truth has eliminated their most painful risk.

Trend 4: Synthetic Identities & The "Phantom Vendor"

The rise of "Synthetic Identity Fraud" involves creating a business that exists on paper but has no physical operations—a "Phantom Vendor." These entities are often backed by real tax IDs and credit histories but are designed solely to extract payment.

- **The "Data Max" Scheme:** An IT director at the Palatka Housing Authority created a fictitious vendor named "Data Max" and approved $155,000 in payments to himself. He used his insider access to onboard the shell company.[4]

Solution: Vendor Self-Verification

To defeat the Phantom Vendor, teams can require the vendor to prove they are real before they can do business. It is not enough to provide valid corporate documents; the individual creating the profile must verify their own identity.

- **Identity Binding:** The vendor representative must upload a government-issued ID and take a live biometric selfie. The system then matches the face to the ID and the ID to the data.

Trend 5: Data Gaps Are Closing

A secure supply chain requires 100% visibility. Procurement teams need to close the "Risk and Data Gap" by applying rigorous verification across the entire supplier spectrum, from massive multinational conglomerates with multiple entities operating in dozens of countries to single-owner vendors who may be tapped 1-2 times a year, while adapting to ever-changing local regulations to ensure speed, accuracy, and security.

- **The "Single-Owner" Dilemma:** Fraudsters often target the "tail spend"—smaller vendors that typically receive less scrutiny. They can slip under automated approval thresholds and more easily penetrate security in small businesses to manipulate payment info and fabricate invoices.

- **Fake Subsidiaries:** Fraudsters can create fake businesses that appear to be subsidiaries of veritable complex corporations. In 2019, a fraudster registered a company in Latvia called "Quanta Computer Hardware." This mimicked Google's legitimate vendor, the Taiwan-based "Quanta Computer Inc." He sent invoices for millions of dollars. Google's staff, seeing the familiar name "Quanta," assumed it was a legitimate subsidiary and paid the invoices for two years.[5]

Solution: Scaled Verification

By implementing an identity-based verification process, teams can create a scalable solution that identifies and prevents fraud for any size of business.

- **Identity Verification:** Systems like Graphite automatically cross-reference the individual owner's Tax ID (SSN/EIN) with IRS records. This ensures that even the smallest consultant is a verified, real person, preventing phantom vendor schemes and small-business security breaches.

- **Enterprise Hierarchy Validation:** For large organizations, complex validations such as live biometric authentications are necessary for corporate hierarchies and parent-child relationships. This ensures that the entities being paid are the authorized subsidiaries and not a spoofed lookalike.

Trend 6: More Countries, More Problems

The speed of business is increasing, and that requires procurement to source from new countries they may have no experience with, and add new vendors faster than ever before. Unfortunately, this creates more opportunity for vendor fraud.

- **Localized Data Validation:** Whether it's verifying a VAT number in the UK, a GST registration in India, or banking rails in Germany, teams need a system that applies **country-specific logic.** This ensures that compliance data is accurate according to local laws, preventing costly cross-border payment errors and ensuring a unified data architecture in your vendor master.

- **Automated Global Compliance:** Teams must adjust supplier questionnaires to trigger relevant compliance checks (e.g., GDPR for Europe, Modern Slavery Act for Australia), to onboard suppliers in new regions quickly without waiting for manual legal review.

Do It All with Graphite

As bad actors develop more effective tools and strategies for manipulating data and accessing payments, procurement teams are struggling to keep up. New risk management procedures are being added to an already full and complicated to-do list for each team member, resulting in an even greater risk of causing a bottleneck and disrupting operations.

That’s where Graphite comes in. Graphite manages supplier verification so your team can focus on strategic projects rather than administrative bottlenecks. By automating a "Verify, then Trust" architecture, Graphite neutralizes the specific threats of 2026:

- **Defeat Deepfakes:** Use **Live Identity Verification and Liveness Detection** to anchor digital actions to physical biology, ensuring users are real humans rather than AI clones.

- **Prevent Account Takeover & Bank Fraud:** Enforce a robust **Bank Validation Waterfall,** including **Dual Authorization** and **Real-Time Rail Validation,** to ensure compromised credentials cannot silently redirect funds, neutralizing the "Insider" Account Takeover risk.

- **Eliminate Synthetic & Phantom Vendors:** Block fictitious entities by requiring **Identity Binding,** which matches a vendor's live biometric selfie to a government-issued ID to prove they actually exist.

- **Secure Agentic AI Workflows:** Maintain a **"Golden Record"** of verified, immutable supplier data to serve as a safety net that prevents AI agents from executing invisible attacks, data poisoning, or unauthorized alterations without human oversight.

- **Bridge the Global Compliance Gap:** Automate **country-specific logic** for data validation and compliance checks to secure every supplier, regardless of their international location.

- **Network Protection:** Leverage a global network to confirm bank accounts have been successfully paid by other buyers, adding an extra layer of collective security.

The Trifecta: Speed, Accuracy, and Security

By automating these localized and tiered verification processes, Graphite delivers:

- **Speed:** Reducing supplier onboarding time by up to **85%.**
- **Accuracy:** Replacing manual data entry and "fat-finger" errors with validated data pulled directly from trusted third-party sources.
- **Security:** Ensuring that every supplier, regardless of size or location, has passed a standardized, rigorous security "fence" before receiving a single dollar.

Conclusion: Winning the Race to Trust

The events of 2024 and 2025 prove that the "Authenticity Crisis" is the defining challenge of our time. Bad actors are using 21st-century technology to exploit 20th-century trust models. To secure the future, procurement leaders must:

1. **Implement "Zero Trust" Data Management:** Remove manual data entry from the ERP.
2. **Build Safeguards:** Build checkpoints and maintain a human presence in automated operations.
3. **Leverage Secure Validation:** Implement tools that quickly and accurately identify whether banking information is correct.
4. **Deploy Biometric Defenses:** Use tools like Graphite to force vendors to self-verify their physical identity.
5. **Standardize Verification:** Develop a process for verification that effectively scales from single-owner businesses to multi-level corporations.
6. **Bridge the Global Gap:** Automate country-specific verification to secure every supplier, from the sole proprietor to the global enterprise.

By adopting a risk-focused architecture, procurement stops being the victim of sophisticated fraud and starts being the architect of a secure, resilient supply chain.

Works cited

1. Cybercrime: Lessons learned from a $25m deepfake attack - The World Economic Forum, accessed November 25, 2025, https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

2. Investigative Report Synopsis - Baltimore City Inspector General, accessed November 25, 2025, https://oig.baltimorecity.gov/sites/default/files/25-0028-I%20%20R.pdf

3. Cleveland Public LIbrary recovers nearly $400K lost in vendor payment scam, https://www.cleveland.com/open/2025/09/cleveland-public-library-recovers-nearly-400k-lost-in-vendor-payment-scam.html

4. Former Palatka Housing Authority Employee Pleads Guilty To Theft Of Federal Funds, accessed November 25, 2025, https://www.justice.gov/usao-mdfl/pr/former-palatka-housing-authority-employee-pleads-guilty-theft-federal-funds

5. US: Extradited Lithuanian Man Pleads Not Guilty in US $100 million Fraud Case, https://www.occrp.org/en/news/us-extradited-lithuanian-man-pleads-not-guilty-in-us-100-million-fraud-case