graphite® Connect

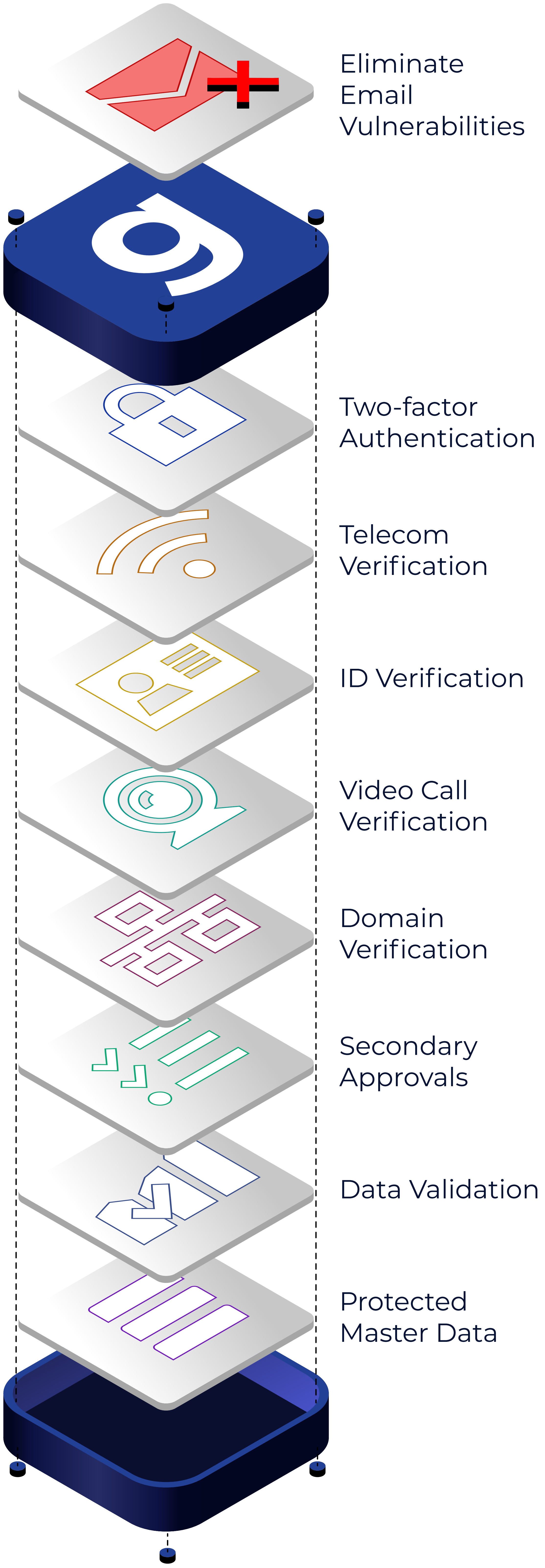
Protect your company from fraud with Graphite Connect

Summary

The growing risk of fraudulent payments from erroneous banking information is a significant threat. Bad actors utilize various attack vectors such as spoofed emails and compromised accounts to deceive businesses and access sensitive data. Graphite Connect is the sole solution for preventing such attacks, employing a Know-Your-Supplier approach coupled with enhanced data validation measures.

Layered Security Approach

Graphite Connect uses multiple layers of security, approvals, and validations to safeguard against attacks. These security layers ensure that only authorized users have access to sensitive data.



Eliminate Email Vulnerabilities

Two-factor Authentication

Telecom Verification

ID Verification

Video Call Verification

Domain Verification

Secondary Approvals

Data Validation

Protected Master Data

Graphite Connect Security and Validation Overview

1. Eliminated Email Vulnerabilities

Email is weak to spoofing and attacks, making it unsafe for identity verification. Graphite uses more secure, reliable methods to verify users' identities.

2. Two-factor Authentication (2FA)

Users must enable two-factor authentication or use a mobile authentication application during sign-up to secure their accounts.

3. Telecom Verification

In supported regions, users verify through a telecom check. This check compares users' phone numbers to public data, verifies their IP, and confirms possession.

4. ID Verification

Users without mobile 2FA or in unsupported telecom regions perform an ID verification. Our user-friendly system quickly confirms identity with valid identification and a selfie.

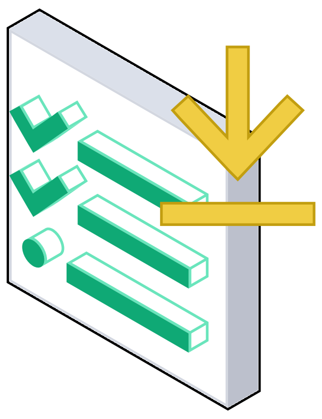
5. Video Call Verification

Users unable to verify through telecom or ID verification instead verify their identity with our global support team via video call. Any high-risk situations are elevated to the requesting company's team for their review.

6. Domain Verification

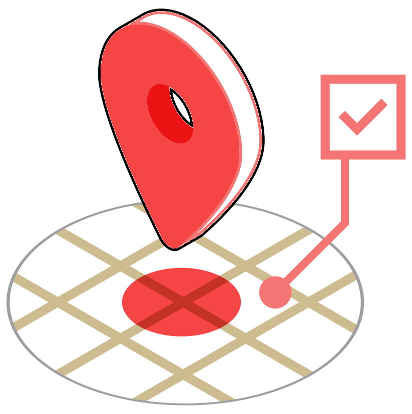
After verifying identity, Graphite validates supplier email addresses to ensure they match the owned domains of the supplier in question. Graphite uses enriched third-party data to not only identify multiple valid domains, but also any relevant security concerns.

Graphite Connect Security and Validation Overview



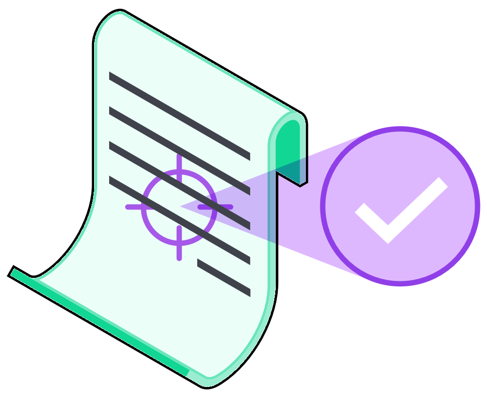
7. Secondary Approvals for Larger Organizations

For larger organizations, a second authorized user is required to review and approve all changes to sensitive data.



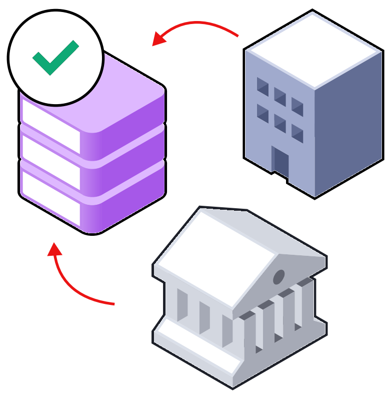
8. Location Data Validation

All location data is verified through third-party data validations. Any non-matches are examined by our validations team.



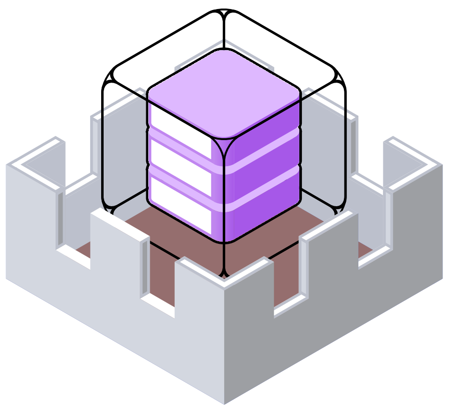
9. Tax Data Validation

Graphite uses advanced Optical Character Recognition (OCR) technology to check tax data and documentation for accuracy.



10. Bank validation

Graphite leverages OCR technology and data verification tools to ensure that supplier banking information is accurate and secure.



✓ **Protected Master Data**

Conclusion

Protection from supplier fraud requires diligent measures and updated tools. Here's how you can establish robust security protocols to safeguard the integrity of your master database's bank and payment data:

1. **Streamline Business Processes and Tools**

   Ensure that your business processes and tools are up-to-date to eliminate manual updates to business data. Reject manual update requests and instead direct connected companies to update their bank data within Graphite Connect.

2. **Implement 2FA and Identity Verification**

   If a bad actor gains access to a company connected to yours, two-factor authentication blocks access to sensitive data. Critical data such as user information, Personally Identifiable Information (PII), and banking data remain secured and inaccessible until users successfully verify their identity through a second authentication method.

3. **Validate Data and Regularly Review Banking Data Updates**

   Validation of bank data is critical. It’s not only important to ensure that data hasn’t been manipulated by bad actors, but also important to confirm there are no data entry errors. Use Graphite to review all banking data provided by connected companies. Graphite notifies your team about changes to connected companies’ sensitive data so you can review and approve the data before it enters your systems.

Graphite Connect provides industry-leading security for business data. To to learn how we can safeguard your company or for more information or to schedule a demo, reach out to us at **sales@graphiteconnect.com** or **(385) 330-1913**.

Request a demo