

Spend Matters™

RESEARCH

CORONAVIRUS RESPONSE: Fraud, P2P and Vendor Management Safeguards — Protecting cash and rapidly vetting suppliers in a crisis

By: Nick Heinzmann

In this installment of our "Coronavirus Response" series, Spend Matters will explore fraud, P2P and vendor management safeguards. With the COVID-19 crisis creating new fires for procurement to put out and critical supply risks arising to address, fraud is an unfortunate reality that businesses need to remain on guard against — especially in times where bad actors mobilize to take advantage of distracted and newly remote operations. This PRO brief will focus on the first solution provider in this category, APEX Analytix.

The mission of this series is to examine categories of relevant solutions and example providers that professionals in procurement, finance and supply chain organizations should investigate to reduce, and even mitigate, coronavirus supply risk. And even if the solutions are only addressing a subset of the issues, the ability to respond intelligently in the short term can also help set organizations up for the future when sanity returns to the world.

Today's brief focuses on the fifth of the seven solution categories that we're covering:

1. **Supply risk management** solutions that include supply chain risk, CSR risk, supplier financial risk, etc.
2. **Sourcing and commodity management**, including advanced sourcing, direct sourcing, automated supplier discovery, and commodity management to help dynamically plan and source. (See this category's recommended solutions for direct sourcing here.)
3. **Advanced procurement analytics** to enable direct procurement and/or to perform "spend planning" when demand drops out or spikes. (Its profile for this series is here.)
4. **Procure to Pay (P2P)** that emphasizes working capital, dynamic discounting, payment control and related finance priorities to help inject cash into the P2P process — especially for many cash-starved suppliers. (This category is discussed in-depth here.)
5. **Fraud, P2P and vendor management safeguards** when new suppliers need to be set up quickly, and also when lowlife fraudsters try to use the pandemic as a way to steal money and IP.
6. **Providers with deep contract analytics** that can analyze a contract portfolio for affected contracts from suppliers (and customers) for not just force majeure clauses, but other related clauses that tie to the multiple risks popping up at once in the pandemic.
7. **Contingent Workforce and Services** solutions that are able to, at a minimum, help rapidly ramp up on-demand workers to deal with massive resource shortfalls. We are looking at four categories of solutions for sourcing remote/online work; solutions for sourcing and managing contract workers at geo-specific capabilities; solutions to "direct source" and manage contract

workers; solutions for data management and analytics. (The first PRO brief from this category, about sourcing remote/online work, can be read here.)

Owing to the magnitude of the crisis, Spend Matters recently made the series introduction available for free to all readers. PRO subscribers can see our follow-up pieces that profile the other categories and their solutions in that market. We will include a lot of information on each category PRO brief that readers can see without hitting a paywall, but since we also draw heavily from our existing deep-dive analysis of the providers from our SolutionMap database, some information will be available only to our PRO subscribers.

For fraud and vendor safeguards, the immediate need for companies in all sectors will include proactively detecting fraudulent behavior from all possible sources, whether it's employees abusing normal corporate channels (e.g., stocking their own homes with toilet paper on the company dime) or cybercriminals posing as suppliers to reroute payments into personal bank accounts. At the same time, manufacturers may need to identify new sources of supply, leading them to rapidly onboard new suppliers. Yet without proper safeguards in place, a frantic selection could lead to longer-term problems, should the supplier have past issues with regulatory compliance or run an unsustainable operation.

Each category-specific PRO piece in this series has three sections:

1. **Problems and Use Cases.** We'll highlight the problems in force (which will vary through different phases of the crisis) and the various scenarios where solutions can provide deeper insights, intelligence and scalable workflows.
2. **Solution Rationale and Value.** We'll outline how various solutions can help solve the problems and the specific questions that they'll help answer.
3. **Example Providers.** We'll highlight the solution providers that can support the problems and deliver value.

Some providers are offering coronavirus-specific programs and "freemium" commercial offers, and we'll note those whenever we update this piece. We'll also start the series with providers that we already have deep knowledge on, but we've been seeking information from other vendors too.

Let's jump into how fraud and vendor safeguard solutions can help.

Problems and Use Cases

The risks of managing spend and suppliers in the COVID-19 crisis fall into two types: compliance and fraud.

- Compliant spending has to do with the control of purchasing processes and internal stakeholders by businesses to drive desired behaviors and outcomes.
- Fraud commonly involves asset misappropriation — when employees or third parties steal monetary or other assets from a business.

Compliance is a critical but simpler issue. With revenue forecasts up in the air and uncertainty dominating markets, businesses of all sizes need to clamp down spending to only the essentials. The en masse movement to remote working should make this easy in some categories (e.g., no more T&E for client dinners or ground transportation) but trickier in others (e.g., do employees really need that Slack subscription they're pushing for, or do current IT investments like Google for Work offer a substitute that the company already has access to?).

Compliant spending also can mean measuring purchases against laws and regulations, and here the pandemic's potential push for businesses to rapidly onboard suppliers could create issues. Supply assurances and affordability may seem like the only concerns, but adding a supplier that is on a denied-party list or has a major stain on its record (e.g., a recent regulatory violation) could only add another fire to put out among the numerous others raging.

Fraud, in contrast, constitutes a wide amount of activity and risks. This is the kind of behavior one hates to see but unfortunately expects in a crisis, especially as employees adjust to the challenges of a remote work environment and numerous other issues compete for executives' immediate attention.

Sources of fraud can include:

- Internal stakeholders could use corporate channels for inappropriate reasons. This could range from using a corporate account to buy toilet paper from a distributor to submitting false expenses or invoices (e.g., non-incurred expenses, re-billed duplicate expenses) to replace lost income from a furloughed spouse.
- Senior internal stakeholders have additional powers that allow them to execute more complicated fraudulent behavior. For example, they can bypass or "rubber stamp" approval processes that would normally catch false expenses or invoices, or their position as a representative of the company can help them construct elaborate schemes (e.g., setting up a shell company between the business and a supplier that collects payments for valid invoices and received goods).
- A vendor in distress looking for cash or a bad actor working for a supplier has numerous means to steal money from a business. Example types of fraud include duplicate/double billing, over-contract pricing and billing for undelivered products or services
- **Third parties (non-suppliers).** Cybercriminals don't wear ski masks; they imitate other people or entities online. Hackers can infiltrate corporate systems in a number of ways, such as phishing scams or gaining access to an employee's unsecured network at home to enter a cloud-based solution. Once they gain access to valid credentials, criminals can create expenses or invoices that appear to be real, or change banking information to route payments to personal accounts.

Solution Rationale and Value

To mitigate compliance issues and fraud risks, procurement organizations need technology that can detect and continuously monitor source data systems for the kinds of behavior described above. In particular, fraud analytics — which uses analytical techniques to analyze enterprise systems and databases to identify vulnerabilities — is of perhaps the most importance, typically for use cases in T&E and invoice fraud.

In the P2P realm, spend compliance and fraud risks stem from poor controls and communication between departments. At many companies, AP processes are still manually managed and paper-based. There also is little coordination between AP and other functions — the former often learns of the expense only when it receives the invoice. In each of these scenarios, the problem is that there's no verification the invoice matches the PO or even if the items/services were delivered.

To combat this, solution providers can use m-way matching that integrates data from multiple systems so that expenses and invoices are properly matched to POs, goods receipts, contracts and the like. Additionally, some vendors make use of machine learning and semantic reasoning to bring unstructured data into the matching process (e.g., text from emails), opening further troves of data for validation.

Pattern and outlier detection is also another route for fraud detection. Remember that the vast majority of purchases are actually valid, so these systems are working to detect the 1% or fewer cases where fraud may exist (or whether a true exception has arisen). Machine learning can be applied to past purchasing behavior to create a baseline of "normal" so that aberrations are immediately singled out for analysis.

Finally, in the case of rapid onboarding for new vendors, risk detection and prevention are paramount. Several vendors offer capabilities to ensure that major risks (e.g., regulatory violations) are surfaced before beginning a relationship, or that when a new supplier has been chosen that the information provided is indeed valid.

The solution use cases described above can help answer questions including :

- Is the supplier a valid entity? And one that you can safely do business with?
- Is the individual representing the supplier or entity they are claiming to?
- Is the email or the obviously incomplete invoice / order acknowledgement you received a phishing scam?
- Is the supplier trying to take advantage of the circumstance and price gouge? And, if so, are they violating a contract?
- How do I protect AP/GL when setting up new suppliers quickly and cutting checks / doing ACHs/wire for emergency funding?
- Is the invoice completely legit? (Fraudsters will try to intercept valid invoices, alter banking / payment info, and resubmit with "correction.")
- How do well-intentioned employees trying to supply their offices (or non well-intentioned employees trying to stock their homes) buying non-approved items affect cash flow and organizational finances?
- Should you limit to approved catalogs or buying portals (such as Amazon Business)?

APEX Analytix

A veteran of the fraud-detection market, APEX Analytix started out as a provider of AP audit recovery services before branching out to deliver an overpayment prevention and self-audit application (Firststrike), procurement fraud risk analysis solutions (FraudDetect) and P2P analytics tools. APEX Analytix also extended its solution reach into the depths of supplier information management (SIM), especially as it relates to the complexities around global supplier onboarding and international compliance management, as well as supplier identity and fraud risk management.

The APEX Analytix supplier management platform focuses on in-depth supplier data collection and management, with additional modules to include dynamic discounting, invoice inquiry, e-invoicing and contract management, supplier statement management and a secure open adapter for integrations to any ERP or P2P-related system (P2P automation, OCR, workflow, compliance). Much of the product emphasis is on identifying and managing supplier and financial information. Like many best-of-breed supplier relationship management platforms, the solution can be tailored to collect and maintain precisely what information the organization needs on the supplier in question, with workflows that depend on the supplier industry, products, services, geography and risk factors.

Core Capabilities

- **Supplier Registration and Onboarding.** In onboarding, APEX takes suppliers through a client-defined registration process that collects the data required by the client organization, in a well-defined order, inclusive of branching workflows should the supplier specify they offer products or services, use certain raw materials or operate in certain geographies in which an APEX

Analytix customer wants to collect additional compliance or related information on the vendor.

- **Financial Information Verification and Controls.** As a SIM solution, APEX can incorporate different payment methods, transfers and controls (and required integrations); provide capture and validation services for SWIFT codes, IBAN codes and bank account numbers on a global basis; offer validation services for any vendor bank account to all required fields and structure (e.g., whether routing information is in the correct format); provide extended validation services (e.g., verifying if the routing information provided for transfers is correct); and validate bank account ownership
- **Rules Editor.** The solution contains a powerful rules (and workflow) editor that makes it easy to define branches in the process and rules for verifying each piece of data that enters the system. For each page, it is easy to add fields, define attributes and specify verification rules that can limit the field to types, values and patterns (as defined by regular expressions).
- **Supplier Portal.** APEX's supplier portal is designed for ease of use and walks a supplier through precisely what information they have to provide during onboarding, making it easy for them to access communications, payment status and other information shared by the buyer.

What Makes It Different

- **Best-in-Class Supplier and Financial Information Validation Capabilities.** The platform integrates with more than 650 global government, regulatory and authoritative data sources, including the standards (e.g., D&B), industry-specific validations (e.g., FACIS) and government validations (e.g., U.S. SAM). This list also includes 250 country address lists, 230 politically exposed person lists, 90 prohibited watch lists, 56 country tax ID/VAT ID lists, 54 secretary of state sites, global banking system validation databases (e.g., ABA, SWIFT, IBAN, IFSC), bank account ownership validation (U.S. and U.K.), industry code and company information databases (e.g., D&B), a corporate linkage database, and the U.S. SBA database. In total, the solution comes preloaded with more than 180,000 validation rules (not a typo).
- **Workflow Configuration and Rules Engine.** APEX Analytix excels not only at collecting and validating supplier information but also in using that information to guide compliance processes and guard against fraud. The system's powerful rules and workflow editor make it easy to define branches in the process and rules for verifying each piece of data that enters the system. The solution enables users to create validation rules down to the individual field level, define them with arbitrary regular expressions, define extensive field lists, define cross-validations, and use them to trigger additional sub-workflows and validations. These capabilities are only matched by a few providers, and primarily providers that also have deep analytics solutions.
- **Top-Performing Risk Modeling and Monitoring Capabilities.** APEX Analytix provides a range of out-of-the-box reporting dashboards that are designed to help an organization monitor the on-boarding process; track and report on key processes and associated metrics; and define bottlenecks to speed up onboarding and approvals. Process monitoring capabilities include audit reports, communication history reports, supplier aging reports, risk monitoring reports and supplier lifecycle reports.

COVID-19 Use Cases

APEX Analytix is a strong fit for any organization looking to rapidly onboard suppliers and keep supplier information current/valid. The total 180,000 validation rules outpace the competition for thoroughness, and extensive configuration of validation and verification rules allows organizations to facilitate granular supplier data gathering and maintenance. APEX's portal also serves as a dedicated hub for suppliers to access a buyer's S2P ecosystem, simplifying the interactions needed for various tasks.

With respect to COVID-19, procurement needs to be able to manage supplier information (new or old) in as automated of a fashion as possible. APEX allows them to do that and more, building a foundation for continuously monitoring the supply base for fraud (e.g., changed banking information). The solution can also be used to handle complexities around international compliance management, as it screens vendors for the kind of legal and regulatory compliance issues that could be forgotten in a hasty selection.