Intelleges

CASE STUDY

## Company Data

| | |
|---|---|
| **Legal Name:** | Intelleges, Inc. |
| **CAGE Code:** | 1WKQ1 |
| **UEI:** | Z15FRTDNBNG5 |
| **DUNS:** | 027820658 |
| **NAICS:** | 541611 – Administrative & Management Consulting |
| **Website:** | www.intelleges.com |

# Case Study 11: Investigations & Due Diligence - Financial Services Vendor & Third-Party Risk Management

**Industry Problem:** Banks, insurance companies, and financial institutions rely on a vast network of third-party service providers -- from IT vendors and payment processors to consultants and data providers. These third parties introduce significant risk: a vendor's failure or breach can quickly become the bank's problem. The financial services industry has seen high-profile incidents like data breaches caused by third-party software vulnerabilities and compliance violations by outsourced partners. In 2024, the average cost of a data breach for U.S. financial firms hit **\$6.08 million** (one of the highest across industries), and many of those breaches originated at third-party vendors. Regulators (OCC, Federal Reserve, FINRA, etc.) now scrutinize how diligently financial companies manage vendor risk. The core problem is executing thorough investigations and due diligence on vendors both at onboarding and continuously -- sifting through allegations, financial stability checks, cyber assessments, and regulatory compliance -- in a consistent, efficient way. Many firms still rely on questionnaires and annual reviews that are tick-the-box exercises, missing red flags until it's too late. The need for a powerful investigative workflow has never been greater: as one report noted, over **60% of significant data breaches now involve a third-party at some stage**, and regulators have observed rising incidents of outages caused by vendor failures.

**Regulatory & Business Risks:** Third-party risk touches multiple dimensions: **security, operational resilience, compliance, financial stability, and reputational risk**. Regulators have formal guidance (like OCC Bulletin 29-2013 and updates) requiring banks to perform due diligence and ongoing monitoring of vendors. Failure to do so can result in enforcement actions, fines, or being ordered to halt certain partnerships. For example, if a vendor handling customer data isn't properly vetted and they leak information, the bank might face penalties under privacy laws and endure reputational damage. Financial institutions also risk direct losses -- consider a vendor outage preventing bank transactions for hours (leading to lost fees, remediation costs, possibly customer churn). There's also **concentration risk**: many firms discovered they were unknowingly too dependent on one critical vendor, which could become a single point of failure. Due diligence should reveal these issues (like whether multiple banks rely on the same small fintech for a key service without backup). Additionally, regulations like anti-money laundering (AML) and anti-corruption (FCPA) require checking that vendors (especially in foreign jurisdictions) aren't conduits for illegal activities -- a failure there can lead to huge fines. Legal risk aside, **boardrooms are worried**: surveys show a majority of financial CEOs rank third-party risk among their top concerns, given how one vendor's mistake can cause an enterprise-wide crisis. The

challenge is not just initial vetting but continuous oversight -- because a vendor that was fine last year might slip this year (financially, or staff turnover, or new ownership). The sheer volume of vendors (large banks can have tens of thousands) makes manual monitoring impossible without a smart system.

**Everyday Pain Points:** A third-party risk manager at a large bank starts her week with an avalanche of tasks. There's a new fintech vendor onboarding to provide a mobile app feature -- she must gather due diligence documents: SOC 2 report, penetration test results, financial statements, compliance attestations... She emails the fintech's contact, who responds days later with some PDFs. She then manually fills a risk assessment spreadsheet: rating the vendor on cyber controls, data handling, disaster recovery. It's largely subjective and information may be incomplete, but business is pushing to onboard fast. Simultaneously, existing vendors need annual reviews; alerts come in -- one vendor was just mentioned in a lawsuit for a data leak, another got acquired by a company in a country the bank normally avoids. She has to investigate these: searching news, asking the vendor questions, possibly escalating to legal or audit teams. It's detective work with limited tools: lots of browser searches, maybe a subscription to an adverse media database. For one critical cloud provider, the bank has a 300-question assessment to update -- she sends it out via email and hopes to get it back complete; if not, she'll chase for weeks. Meanwhile, auditors (internal or external) ask for evidence of vendor oversight: she scrambles to find last year's assessment files for a particular vendor, digging through network folders. The process is stressful, inconsistent, and prone to gaps -- which keeps her up at night worrying "What am I missing? Have we checked all our vendors against sanctions lists recently? What about fourth parties (the vendors of our vendors)?" Without an integrated system, crucial intel (like a small IT vendor's CEO was convicted of fraud, hypothetically) might not reach her unless by chance. And if a front-line business owner decides to engage a contractor without looping her team in, that vendor might fly under the radar until a problem arises. It's a precarious situation where despite best efforts, the house could come down if one hidden risk isn't caught.

**Intelleges Solution -- Protocol & Workflow:** Intelleges offers a robust **Third-Party Investigation & Due Diligence Protocol** that centralizes and automates vendor risk management in financial services. The platform acts as a unified hub where *all vendor data, risk scoring, and investigation workflows reside*, replacing the patchwork of spreadsheets, emails, and siloed databases. The **6-step Protocol Workflow for Vendor Due Diligence** works in concert with an ongoing monitoring loop:

1. **Onboarding Due Diligence Intake:** When a new vendor or

third-party is proposed, Intelleges initiates a structured due diligence request. It dynamically tailors the scope based on vendor type, criticality, and inherent risk (for example, a vendor processing customer account data triggers a deep dive on cybersecurity and privacy, while a low-risk office supplies vendor gets a lighter check). The system sends the vendor a secure link to a comprehensive questionnaire -- covering everything from financial health to compliance controls. Because Intelleges has **26+ harmonized questionnaires for different standards**, it picks the relevant ones (e.g. a cloud IT provider might get a combined ISO 27001/CIS Controls questionnaire). The vendor can upload supporting documents directly: SOC reports, ISO certs, policies, etc. No more email ping-pong; all required info is gathered in one workflow. Intelleges also automatically pulls baseline data: corporate registration details, any available credit scores or financial ratings, litigation history (by integrating with legal databases), and sanctions list checks (screening the vendor and key principals against OFAC, politically exposed persons lists, etc.). This step essentially creates a digital dossier on the vendor.

2. **Risk Scoring & Analysis:** Once data is in, Intelleges analyzes it

to produce initial risk scores across multiple risk domains: cyber risk, data privacy risk, financial viability, compliance risk (AML/KYC), operational resiliency, etc. For example, if the vendor's SOC 2 report shows several sub-optimal findings, the cyber risk score might be moderate-high. Or if their financial statements (or credit rating) are weak, the financial risk is high. The platform applies internal risk models that can incorporate industry benchmarking too -- comparing the vendor's responses to what similar vendors typically have. If the vendor operates in, say, a high-risk country or uses sub-contractors, those factors weigh in. This quantitative scoring is combined with flags: *"No evidence of business continuity plan -- flagged"*, *"Pending litigation detected -- flagged"*. The system might highlight: *Vendor X has a breach history (found via dark web or news search), be cautious*. All of this gives the risk manager a clear, data-driven view rather than relying on gut feeling. Notably, Intelleges can incorporate **FINRA observations or regulatory guidance** as rules -- e.g., FINRA noted increased third-party outages, so the presence/absence of a robust incident response plan will affect the score.

3. **Cross-Functional Review & Approval:** Intelleges routes the

collated analysis to relevant stakeholders for review. Legal might look at contract terms and any legal flags, InfoSec reviews the technical controls, Business Owner confirms the vendor's strategic fit, etc. The platform provides a dashboard where each reviewer can see the highlights and dive into details if needed (for instance, clicking to read the SOC 2 report or the actual adverse media excerpts). They can comment or ask follow-up questions right in the system, which then loops back to the vendor if necessary. This replaces endless meetings or email threads; everyone is literally on the same page. If follow-ups are needed (say InfoSec asks the vendor for clarification on encryption practices), Intelleges manages that Q&A. Finally, the risk manager or a committee uses all this input to decide -- approve, approve with conditions (e.g. vendor must fix certain issues within 3 months), or reject. Intelleges records the decision and reasoning. This documented review process is crucial for regulators: it proves the institution has a consistent due diligence process. And Intelleges can automatically generate an **"Approval Memo"** with the key points and sign-offs, saving manual documentation effort.

4. **Contractual & Control Obligations Tracking:** Once a vendor is

onboarded (approved), Intelleges ensures that all agreed risk mitigations are put in place. If during diligence the bank decided "Vendor must maintain cyber insurance of \$X and undergo quarterly vulnerability scans," Intelleges will incorporate those into the vendor's profile and set reminders or workflows to obtain evidence of compliance (like uploading the renewed insurance certificate each year, or results of scans). It might also feed requirements to the contract management: some clients integrate Intelleges with their contract systems so that any conditions are explicitly written into the contract. By tracking obligations, the platform makes sure the due diligence doesn't become a one-time checkbox -- the vendor is continually held to the specific controls promised.

5. **Continuous Monitoring & Alerts:** After onboarding, Intelleges

goes into monitoring mode. It continuously ingests relevant data about the vendor: news feeds (scanning for the vendor's name in news of breaches, fines, mergers, etc.), regulatory watch lists, performance data (like SLA metrics the vendor is measured on), and even **fourth-party information** if available (some vendors share who their critical suppliers are; Intelleges can monitor those too). If anything significant occurs, the system creates an alert. For instance, *"Vendor Y's average response time has degraded beyond SLA for 2 months"* (operational risk), or *"Regulator issued a warning about a practice related to what Vendor Y does"*, or *"Vendor Y's CEO resigned abruptly -- potential instability"*. One tangible example: in 2025, multiple banks were caught off-guard by a breach at a major cloud service provider -- with Intelleges, the moment that breach hit news, every client using that provider would get an alert and a suggested action (e.g. "Contact vendor for incident report, evaluate

compensating controls"). This real-time aspect transforms vendor risk from periodic hindsight to ongoing oversight.

6. **Investigation & Issue Resolution (Adaptive Workflow):** If an

alert or incident occurs, or if periodic review time comes, Intelleges launches an investigation workflow (leveraging its 7-step verification process in complex cases). For small issues, it might be just a task to the vendor manager: "Follow up on Issue X and document response." For larger issues -- say a vendor experiences a data breach -- Intelleges would escalate to a full case: gathering details, assessing impact on the bank's data, ensuring vendor takes remediation, possibly requiring the vendor to undergo a fresh risk assessment. The platform ensures accountability: issues are assigned, tracked, and resolved or escalated. For instance, if a critical vendor is acquired by a foreign company, the system might require a re-do of due diligence under the new ownership. All actions are logged, so if regulators later ask "How did you respond to that vendor's breach?", the bank can produce a timeline of exactly what was done (e.g. cut off access within 2 hours, obtained root cause report in 5 days, independent security audit done in 30 days, etc.). This step is essentially Intelleges adapting and enforcing the vendor governance lifecycle.

Throughout all steps, Intelleges provides a unified repository: every vendor's complete "risk file" is in one place. So producing reports for auditors or senior management is straightforward. Need a list of all high-risk vendors with missing documentation? One click. Need to show the board the top third-party risks and what's being done? Dashboards are ready, with drill-down capability.

**Real-world Results:** Financial institutions using Intelleges have reported transformative outcomes. A large regional bank with around 1,000 active third-party relationships managed to **reduce its vendor onboarding time by 40%** -- from an average of 10 weeks down to 6 -- while *improving* thoroughness. This meant faster time to deploy new fintech partnerships, giving them a competitive edge in launching new digital services, without sacrificing risk controls. Another firm credits Intelleges with slashing the effort of annual vendor reviews: what used to occupy a team of five for months (chasing questionnaires, compiling reports) is now largely automated, allowing the team to focus on analyzing and mitigating risk rather than clerical work. Critically, Intelleges has helped organizations catch issues that would have otherwise slipped by. For example, one bank discovered through Intelleges' monitoring that a small IT contractor they used was **implicated in a separate company's fraud case**. Intelleges flagged the adverse media, prompting the bank to pause and investigate -- they ultimately decided to disengage that contractor, potentially avoiding being entangled in a scandal. In the realm of cybersecurity, companies have seen measurable risk reduction: one insurer noted that before Intelleges, about 30% of vendors had at least one unchecked compliance item (like missing security training documentation or outdated certs); after a year with Intelleges, they drove that to near 0%, because the system simply didn't allow neglect -- automated reminders and escalations saw to that. Impressively, when regulators came knocking, these companies could demonstrate robust programs. A compliance officer at a wealth management firm recounted how, during an exam, they quickly generated reports from Intelleges showing every vendor's risk rating, last assessment date, next planned action, etc., which *"greatly satisfied the examiners"* and resulted in zero findings related to third-party risk (contrasting with peers who often get cited in that area). Quantitatively, avoiding breaches and disruptions is hard to measure until something happens, but one can point to industry stats: those using such proactive vendor risk tools tend to avoid the multimillion-dollar breaches others suffer. Indeed, in an analysis, financial firms with strong TPRM (Third Party Risk Management) programs have 72% less likelihood of a severe vendor-related incident -- Intelleges essentially operationalizes that strength.

**Why Intelleges -- The Right Fit for Any Size Financial Institution:** Intelleges proves its value whether the organization is a global bank or a smaller fintech startup. **Large**

**enterprises** benefit from the platform's scalability and integration -- it can handle tens of thousands of vendors, tie into existing GRC (Governance, Risk, Compliance) systems and threat intel feeds, and enforce enterprise-wide policy uniformly across business units and geographies. The result is no more gaps where one region did minimal checks and another did thorough ones -- everyone uses the same best-in-class process. And the analytics at scale (like comparing risk scores across divisions or flagging systemic fourth-party risks) are immensely valuable for strategic risk planning at the top level. For **mid-market or small financial companies**, Intelleges is like a pre-built vendor risk department. They get access to templates and intelligence typically only big banks have (e.g., pre-written assessment questions aligned with the latest regulations, automated screening that normally requires costly data subscriptions). It allows a lean team to manage risk like a large institution, which is particularly important as regulators don't necessarily scale expectations by size when it comes to core risk areas. Moreover, Intelleges is **constantly updated** for evolving threats and compliance requirements. For instance, if a new regulation comes out (like Europe's DORA -- Digital Operational Resilience Act -- or new Fed guidance in 2025), Intelleges can incorporate those into its questionnaires and risk logic, keeping clients ahead of the curve. This adaptability means the investment in the platform keeps paying dividends as rules change -- crucial in financial services where regulatory goalposts move frequently.

Finally, Intelleges' holistic approach fosters **trust and transparency**. Internally, business owners and risk managers stop viewing each other as adversaries (one pushing speed, the other caution) because the platform makes the process collaborative and efficient. Externally, vendors even appreciate the clarity -- they know what is expected and can demonstrate their value as "trusted partners" more easily. Over time, Intelleges helps build a resilient ecosystem: it doesn't just evaluate vendors, it often uplifts them (e.g. sharing best practice checklists, prompting them to improve controls to win business). In a world where outsourcing is necessary but risky, Intelleges is the rational solution that makes third-party risk **manageable, measurable, and mitigable** for financial institutions of all sizes. It replaces uncertainty and reactive scrambling with confidence and proactive control, which is exactly what regulators, customers, and shareholders want to see in the financial sector.