A Risk Manager's Story

Understanding the factors that threaten efficient and effective payments management

Summary

Managing risk at a payments company requires comprehensive awareness: Where are you vulnerable? What are your obligations to stakeholders, partners, and legal compliance? Are the processes and tools you use to detect suspicious activity reliable and efficient? Here, a longtime user of G2RS technologies shares his perspective on risk multipliers in the payments industry, how to ward off the "compliance shock" that can come with rapid growth, and the importance of choosing flexible monitoring and detection tools you can tune to your unique requirements.

The challenge

Payments companies are in the business of managing risk. By facilitating payments to a merchant, they take on the very real risk that the process will be mishandled or abused, either through non-compliance with regulations or other agreements, or through nefarious acts like fraud. As such, managing risk around payments requires comprehensive awareness of vulnerabilities.

"Every business in the industry has a different set of areas where they're vulnerable to fraud or non-compliance," says Phil Douglas, a longtime senior risk and compliance manager who has worked at Nium, Paddle, Paysafe, and other organizations that rely on the safe, efficient onboarding of merchant payees. "When it all goes wrong, you can be stuck trying to fix a serious problem while also restoring the faith and confidence of those who rely on your success."

The key, Douglas says, is taking a wide view of the risk and mitigation strategies that apply to your unique business, and equipping yourself with the policies, procedures, and tools required to implement those strategies proactively. If you address risk reactively, a breach can occur that threatens your bottom line, your partners' and stakeholders' confidence, and even the continued operation of your business.

In a **recent webinar,** G2 Risk Solutions (G2RS) invited Douglas to share his perspectives on the issues that fintech companies encounter when implementing effective payments operations. Douglas discussed the complications around risk that occur when a company grows too fast and lacks the tools to address inefficiencies caused by false positives and other faulty alerts. This case study expands on these factors, highlighting key points and illustrating how these risks can lead to catastrophic results when companies fail to anticipate their effects.

Planning for potential risk multipliers in payments operations

Payments risk mitigation largely focuses on the threats of identity theft and transaction laundering—the unauthorized processing of payments by one merchant on behalf of another for deceptive and fraudulent gain. Bad actors succeed in this space by exploiting vulnerabilities in the legal and technological infrastructure of the payments ecosystem, often bypassing expensive software solutions that merchant monitoring teams have put in place. The problem, Douglas says, is always escalating.

"As awareness of a particular payments security product grows, you get more bad actors who are going to circumvent that product to get what they want," he said. "Detection tools must be better than the smartest person who wants to undo them."

> *As awareness of a particular payments security product grows, you get more bad actors who are going to circumvent that product to get what they want. Detection tools must be better than the smartest person who wants to undo them.*
>
> **Phil Douglas**
> Senior risk and compliance manager

And even the best tools won't work if a company's risk policies are in disarray. While keeping one eye on vulnerabilities related to theft and laundering, companies must also pay attention to other risk factors that might affect their business. Douglas points out three key vectors where a merchant's business model impacts payments risk:

- **Product types**
  Merchant risk is clearly associated with the products offered for sale. Lower-risk products, such as clothing or toys, set a low bar for regulatory compliance, while higher-risk models, like online gambling, pose greater risk because there's more "red tape" for payments processors to navigate. However, the lack of regulations around supposedly low-risk merchants also makes them an easy target for scams, because there's less bureaucracy for fraudsters to get around.

- **Delivery methods**
  Merchants that deliver online services present different risks from those that deliver hard goods. In particular, software-as-a-service (SaaS) providers expose payments providers to additional risk because their subscription models make it easy to hijack or subvert online payments without detection in the physical world.

- **Rules**
  Businesses that transact payments via an acquirer are typically beholden to the myriad and complex laws that govern those transactions. Some business models are also heavily accountable to partnership agreements, as is the case with merchants of record (MOR) who establish merchant accounts and underwrite on their behalf, working for acquirers who impose strict expectations and legal requirements of their own.

Amid these nuances in risk management, payments companies have plenty to deal with when doing business. As Douglas points out, the urgency is underscored by the bad actors' ability to overcome technical obstacles.

However, there is yet another factor he identifies as a significant accelerator of risk—the rapid growth of a payments company, where sales outpace risk detection and mitigation.

Anticipating the compliance shock that comes with growth

Almost any business welcomes growth, and the faster they achieve it, the happier they are. This might be especially true for fintech companies, including payments processors. Who in the payments industry doesn't want to see their merchant onboarding numbers exceed expectations?

Growth, however, doesn't just pertain to near-term profits—it pertains to the company as a whole, including its obligations to stakeholders who rely on its continued success. This makes it vital to comply with rules and agreements, whether to government jurisdictions or to the other companies you do business with. When a company grows too fast, it sometimes fails to account for these obligations in time to ward off catastrophe.

Douglas knows this all too well. The same week he joined an MOR as a risk analyst, the company got hit with a Microsoft Tech Support scam that impacted a wide swath of merchant accounts. Even though his new employer had enjoyed significant recent growth, the event jeopardized a key partner's business, and the partner abruptly terminated its contract.

"It was a huge blow to our business," Douglas says. "The partner relationship in question was strategic to our success. In the wake of it, several of my team members left the company, including the person who brought me on."

Not just that, he says, but the blowback across the company's remaining business was severe. Other partners wanted to know what happened, how it happened, and what Douglas' team was doing to make certain it didn't happen again. With crucial partnerships at risk, the business threat was more than chaotic—it was existential.

In this example, the breach escalated in ways that led to compliance shock—the reckoning that takes place when a business' growth exceeds its capacity to meet legal and/or stakeholder obligations. Ultimately, Douglas and his remaining team members found the problem to be one of insufficient awareness and the limitations of their transaction monitoring and detection tools.

"As your company grows, you're expected to have solid policies, procedures, and controls in place, and basically none of that was implemented prior to my arrival," he says. "The company had failed to maintain a compliance environment that met our partners' expectations, even as the onboarding numbers steadily increased."

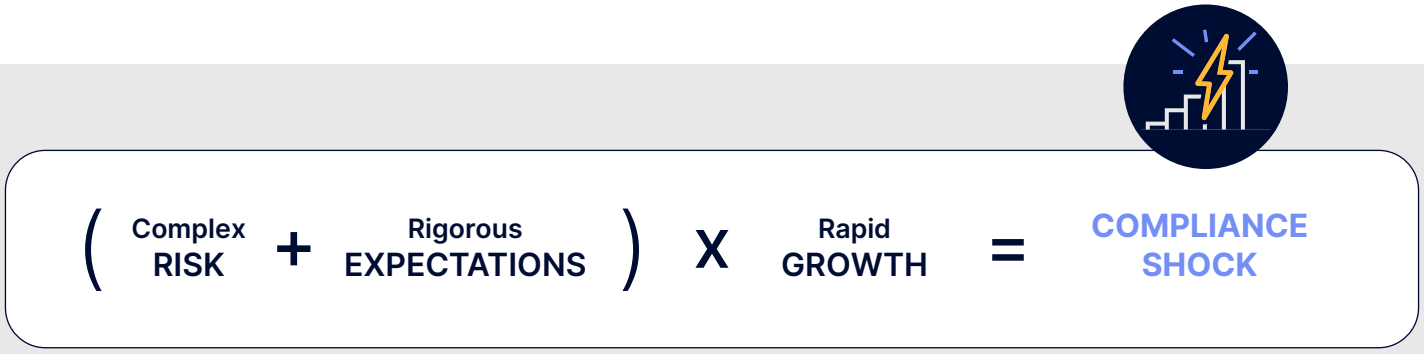

Fig. 1. Compliance shock can result from rapid growth when companies fail to account for underlying business obligations.

Slipping the net: How false positives block effective monitoring and detection

Amid the chaos of compliance shock, there's still the day-to-day business of monitoring transactions to detect non-compliance and fraud. Typically, payments companies use a toolset that examines each transaction and sends an alert to the risk team when something looks suspicious. The team then investigates the problem, assesses the risk and possible damage, and takes action as needed to repair operations.

So far, so good. But the success of that team is bound by many factors, including team size, tool capabilities, an awareness of pertinent rules and regulations, and the ability to prioritize work based on relevance. How important is each alert? Which ones are most important? Why are they important? What response is needed, and what's the urgency of that response?

Unless you're able to manage risk in a way that gives you immediate answers to these questions every time, the efficiency (and ultimately the credibility) of your risk analysis is going to suffer. Success depends not just on timely response to alerts, but also on the quality of those alerts themselves. Your team might have the smartest, most capable risk analysts in the business, but like any modern professional resource, they're always going to be limited by the quality of the data in front of them.

For Douglas, the two biggest data issues are non-alerts and false positives. A "non-alert" takes place when your software fails to detect a potentially harmful anomaly; in that case, the solution you're using is clearly faulty.

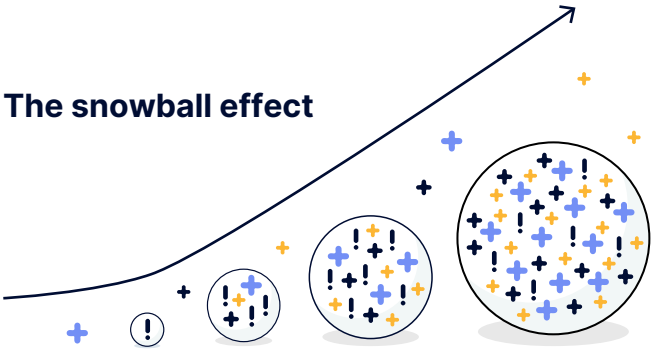

Fig 2. False positives proliferate more quickly when a company experiences rapid growth, leading to slower and less effective operations.

The more insidious and maddening culprits are false positives—alerts that get the attention of your analysts but lack any credible threat. False positives waste valuable time for the team, who must analyze the threat, only to then discard it.

In Douglas' experience, false positives can become a dire problem. "We'd see these alerts and say, this looks like something very serious...but is it real? On what basis is it being detected?" Douglas says. "Do we really need to take action, or is it a bogus alert? If it's bogus—how can we immediately adjust the system's rules so we stop receiving alerts on the same erroneous basis?"

False positives proliferate more quickly when a company experiences rapid growth. "At one company, we implemented self-service onboarding, which was a huge success in terms of adoption," says Douglas. "But the number of alerts shot up from a few hundred per week to over ten thousand in the first month, and the vast majority of those were false positives. With the team size we had, it was impossible to track down every one."

This snowball effect caused Douglas and his team a great deal of alarm. "We knew we had false positives, but we still couldn't afford to ignore any of the alerts, because who knows what kind of bad actor we might let slip the net," he says. "We needed tooling that could keep pace with these activities while also allowing our analysts to interact meaningfully with the alerts and adjust the rules they were based on, as needed, in real-time."

Success depends not just on timely response to alerts, but also on the quality of those alerts themselves. Your team might have the smartest, most capable risk analysts in the business, but like any modern professional resource, they're always going to be limited by the quality of the data in front of them.

Finding solutions that address the right risks at the right times

At the MOR where Douglas saw the breach that cost an essential partnership, inadequate tooling was ultimately to blame, along with the human failure of maintaining risk awareness. Following the breach, awareness was considerably heightened—but the limitations of the toolset still needed to be addressed.

"We had a strong, positive relationship with the account manager at our existing solution provider, but it was clear they couldn't offer the customizations we needed," says Douglas.

Specifically, Douglas and his team needed granular, real-time visibility and control over alerts and the rules they were based on. They needed a fraud detection solution that maintained itself with minimal unnecessary impact on the analysts who used it. And they needed it as soon as possible.

"We didn't have the luxury of conducting a 6-month RFP," says Douglas. "Our remaining partners wanted to see results right away, and so did our team. Some of our key stakeholders favored an alternative provider, but in the end, G2RS was the only company that gave us the flexibility we needed."

G2 Risk Solutions conducted a proof of concept (POC) at Douglas' employer that used configurable rules for both monitoring merchants and detecting laundering instances. When they tested the POC against roughly 2,000 merchants comprising a reported 10-15% of their monitoring portfolio, they achieved the following results:

- **Reduction in workload**
  Previously, alerts (that were mostly false positives) numbered into the thousands per week. The new solution yielded only a few dozen alerts per week.

- **Accuracy of alerts**
  Investigation by Douglas and his team revealed nearly all alerts to be credible threats.

- **Real-time revision of monitoring rules**
  The few alerts that weren't actual threats were easily prevented in future scans by adjusting rules in the toolset.

- **Proof of detection**
  On the detection side, only "real" threats were reported—including alerts based on suspicious data Douglas' team intentionally provided to test the system.

The POC and subsequent conversations with G2RS yielded other helpful features that Douglas' team could easily opt into, including bespoke investigation capabilities based on manually adding URLs, and the ability to train the system to recognize custom, problematic words.

Douglas and his team needed granular, real-time visibility and control over alerts and the rules they were based on. They needed a fraud detection solution that maintained itself with minimal unnecessary impact on the analysts who used it. And they needed it as soon as possible.

The future of risk assessment for payments

As payments companies scale up onboarding, their long-term success depends heavily on shoring up risks. To do this, they need tools, policies, and processes that keep pace with bad actors and business growth.

“Fraud gets more sophisticated, just like technology does,” says Douglas. “High-quality monitoring and detection will always be essential for helping fintech companies get in front of these problems. And because every business is different, it’s vital that they choose flexible tools they can tailor to their operations.”

Once you have that, Douglas says, the benefits are self-evident. “When you manage risk appropriately, you get stronger customer and partner relationships that are secured for a longer duration of time. You spend less on operations and more on revenue-driven activities, enabling your business to become the best that it can.”

About G2 Risk Solutions (G2RS)

G2 Risk Solutions is the definitive expert in risk and compliance business intelligence for financial institutions and online platforms. We are industry pioneers providing market-leading solutions for merchant risk, digital commerce risk, bankruptcy risk, and credit risk and regulatory reporting. We are driving innovation and shaping the future of risk management through unprecedented data, technology, and global compliance and risk expertise, providing the financial services and digital commerce ecosystems with the tools needed to navigate complex and ever-changing regulatory requirements and mitigate risk.

Contact us