KPMG

A triple threat across the Americas: KPMG 2022 Fraud Outlook

Sector Spotlight: Financial Services

Five things financial services executives need to know

KPMG's "A triple threat across the Americas" highlighted the overlapping fraud, non-compliance, and cyber attack challenges that confront businesses across all sectors today. This follow-up piece reviews the dangers facing financial services (FS) companies, and outlines five things that FS executives need to know:

01 FS firms have the most extensive, and expensive, fraud burden of any sector in the Americas.

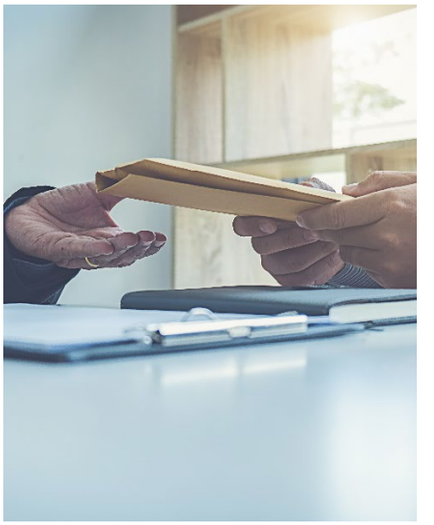
Fraud is the norm rather than the exception everywhere, but it is particularly so in financial services. Fully 85% of FS respondents to our survey reported that their companies experienced at least one fraud in the past year. Over the same period, the known loss to fraud by these companies was the equivalent of 0.6% of annual profits—one quarter higher than the cross-industry average of 0.48%.

"Fully 85% of FS respondents to our survey reported that their companies experienced at least one fraud in the past year. "

02 Insiders, customers, and organized criminals present almost equal fraud threats for FS companies.

Rather than a dominant class of fraudster, companies in this industry need to be prepared for threats to come from almost any direction. One source is those inside the company itself: 34% of FS respondents report a known fraud in the last year perpetrated by one or more of a senior executive, middle manager, or operational employees. Nearly as widespread is the threat from customers or clients, who were behind fraud at 31% of these companies. The same proportion were hit by organized criminals, including cyber criminals.

Looking ahead, the threat environment could worsen: 56% of FS respondents expect the fraud threat from external actors to increase in the coming year, compared to just 17% who see a decrease. Meanwhile, 69% of executives believe that “organized crime remains a substantial challenge to doing business legally,” where they are working. This is well above the cross-industry average, suggesting a particularly elevated risk.



03 Compliance, already a difficult area for FS companies, looks set to get much tougher.

The costs of non-compliance are currently high for the sector. Respondents report that, on average, their firms had to pay the equivalent of 0.54% of profits in fines in the last year, well above the 0.46% cross-industry average. Looking ahead, most FS executives expect these difficulties could grow. Sixty-two percent think that overall compliance risk will rise in the coming year, compared to just 11% who foresee a decline.

Again, rather than a single issue, compliance threats will take multiple forms. In particular, 61% of surveyed industry leaders expect to face new requirements related to data privacy and 45% an increase in international divergence of rules on anti-corruption and anti-money laundering – particularly relevant issues for cross-border FS providers.

Meanwhile, after this survey closed, geopolitical events in Ukraine further complicated compliance for FS in particular. The US plays a critical role in providing the infrastructure for the global financial system. As a result, its extensive and recently imposed sanctions are, in practice, now requirements for almost all sector firms. They will also be rules where the regulatory – and reputational – risks of falling short will be very high.

04 FS companies are experiencing a range of negative impacts from a tidal wave of new cyber-risks.

In the last year, 87% of industry firms saw a rise in at least one kind of cyber attack, the highest figure in our survey for any sector. Phishing (reported by 49%) and scamming (37%) saw the most widespread growth, but more than one in five (21%) financial services business is wrestling with a rising number of ransomware attacks. The resultant damage is not just economic: 31% of survey executives say that a cyber attack triggered a regulatory or compliance investigation at their firm over the last 12 months, and nearly a quarter (23%) that such an IT event led to sustained reputational damage.

Here, too, little respite is in sight: 78% expect cyber-risks to rise. Meanwhile, the US Securities and Exchange Commission is expected to pass a four-day notification requirement for cyber incidents, making the attendant regulatory risk greater still.[1]

[1]"Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Proposed Rule, 9 March 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf

05 In the face of this substantial triple threat, too few companies think that they have strong defenses—and many reveal vulnerabilities.

industry is even larger than the substantial one facing other companies, too many businesses lack the high levels of protection needed. Just 58% believe that their company's network security is somewhat or very mature, for example, while just 31% say that they are extremely effective at finding instances of fraud or non-compliance and at taking action to mitigate the effects of both. Moderately good defences are simply not enough here.

Meanwhile, individual answers give pause for thought. Over half of FS respondents (53%), for example, would not be surprised to hear in the coming year that private customer data leaked from their company; 61% report that they have not effectively updated pre-pandemic fraud controls to reflect the new working reality; only 43% expect to increase investment in improved compliance in the coming year, despite the growing risk of non-compliance and already high cost to the sector; and 28% think that their companies would pay off those behind a ransomware attack should one occur – the highest figure for any industry. Given the current extent of the triple threat, specific weaknesses will be exploited.

KPMG's viewpoint: Make your defenses fit for purpose

The world is always changing but, occasionally, it experiences a dramatic inflection point. The COVID-19 pandemic reset all kinds of assumptions about how people live and work. Now, geopolitical events are exposing the fragilities of people's assumptions about the international environment.

The risk landscape that businesses are grappling with has been similarly reshaped. The need to maintain access to supplies has driven many companies to rely on previously unvetted partners, potentially raising new fraud risks. On compliance, the drive for net zero is expected to create further environmental regulation and new global sanctions may lead to more stringent oversight of financial and trade activity. Finally, cyber attacks, already on the rise during the pandemic, are allowing cyber threat actors to pursue a range of aims.

In short, if your company has not recently conducted a full review of its fraud, compliance, and cyber security risks, it should conduct one as soon as possible. Otherwise, your defenses may not be tailored to combat today's threats, or be able to react as those risks rapidly evolve.

While re-examining the risks is a necessity for every sector, it is especially one for FS companies. In times of economic difficulty, with inflation higher than in many years, people within and outside companies are much more likely to rationalize engaging in fraud. FS will be a prime target for such actors for the same reason it already suffers outsized losses: these crimes are financially motivated, and FS is the sector where most money itself is the focus of business.

The basic framework of prevention, detection, and response remains the soundest foundation for addressing the triple threat of fraud, non-compliance and cyber attack. The environment in which these defenses are deployed, however, means that they should retain the most effective elements and build upon them to defeat evolving threats.

Prevention

In our view, certain elements will remain largely the same, such as implementation or enhancement of internal controls; risk-based integrity due diligence on employees and third-parties; security assessments of critical information systems; and simulated cyber attacks to expose exploitable vulnerabilities. Others are expected to take a new shape. For example, implementing rules on exceptions to vendor due diligence policies may be necessary amid supply-chain shortages, but companies need to balance strategic necessity with the imperative to avoid falling victim to fraud and staying on the right side of regulation.

Detection

We believe tools such as data analytics, internal audits, and cyber intrusion detection protocols will remain fundamental, but the misbehaviors they look for may be different. Moreover, even where more employees are working at home, theirs are the eyes and ears that will see compliance failures or fraud. Measures that companies should take include updated training on fraud and compliance risks, and on the importance of reporting unusual behavior through existing incident-reporting mechanisms

Response

Protocols must be in place to respond to fraud, instances of non-compliance and cyber breaches. Companies also need to be ready for the emerging challenges within today's risk triangle. This might include, for example, deciding ahead of time whether you are willing to pay in the event of being hit by ransomware or choosing in advance who would make that call.

For further information on how KPMG can help you, please contact us:

Thomas P. Keegan
Principal, Forensic
KPMG US

David Nides
Principal, Cyber Security Services
Forensic
KPMG US

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities