Fraud ready

What it is and why it's important

KPMG LLP recently performed a survey[1] which highlighted that the financial services industry has the most extensive, and expensive, fraud burden of any industry sector in the Americas. This probably comes as no surprise after the uptick in fraud during the Covid pandemic. With a recession predicted for 2023, and with fraud often being a crime of opportunity, exacerbated by the economic climate, financial institutions face the situation getting worse before it gets better. In fact, 56% of financial services respondents to our survey expect the fraud threat from external actors to increase in the next year.

Financial institutions are aware of the challenges they face in managing fraud. Fraud, after all, is a risk of doing business as a financial services firm. Whether you're a retail institution offering checking, savings, and credit card products; an insurance company offering policies on assets; or a firm offering loans to individuals and businesses—financial products inherently carry the risk of fraud. However, what has changed for these firms is the fraud landscape:

- Cyber-attacks have increased in number over recent years. In our recent survey, 87% of financial services firms saw a rise in at least one kind of cyber-attack. Cyber-attacks can include malware-based, password, phishing, denial of service, SQL injection and DNS tunnelling attacks. Of them all, phishing attacks saw the most widespread growth, but more than 1 in 5 financial services businesses are wrestling with a growing number of ransomware attacks. While most agree that there has been an increase in cyber-attacks over recent years, it is often debated that the number of attacks is much higher as some go unnoticed or unreported. Bad actors, wishing to get access to accounts and assets, target companies across a multitude of other industries ranging from hospitality to manufacturing, technology to retail, and sports betting to technology. Some companies in these other industries that have not historically made significant investments in information and cyber security are targeted. Customer data from those attacks can be used in a variety of different schemes including the creation of synthetic IDs and leveraging bots and automation to launch credential stuffing at financial services firms. These methods allow the fraudster to access accounts and execute transactions all while masquerading as a legitimate customer. As a result, it is extremely challenging for the financial institution to know who an actual customer of the firm is and who is not.

[1] Source: KPMG LLP, A triple threat across the Americas: KPMG 2022 Fraud Outlook (2022)

- From time to time, financial services firms will experience fraud surges, where the volume of fraud related to a particular scam increases substantially, sometimes leaving Fraud operation teams struggling to keep up. Over the years, fraud surges have been driven by government imposter scams (e.g., IRS scams), romance scams, and online purchase scams. Fraud amongst COVID-19 related benefits, such as Paycheck Protection Program (PPP) and Small Business Administration (SBA) loans, arose during the pandemic and resulted in surges experienced across the financial services industry. Scammers continue to evolve and leverage new and emerging trends, making it challenging for financial institution firms to keep ahead of the threats. In 2023, institutions can expect a continuation of the prevalent scams observed in 2022, along with the emergence of student loan forgiveness scams in response to the current administration's student loan program, as well as second party fraud in response to the anticipated P2P liability shift to banks. In addition, as the cost of everyday items rise, higher rates of promotional abuse, increases in friendly fraud (wherein consumers claim fraud on legitimate transactions that initiate costly chargebacks to businesses), and employee fraud will likely increase because of cost-of-living pressures.
- The pandemic drove a lot of business and personal transaction activity online. Face to face transactions pivoted to virtual payment options and increased the need for delivery of goods and services. This shift resulted in more consumers providing companies with personal identifiable information (PII) to obtain such, either online or through newly established eCommerce capabilities. New digital payment types (e.g., "tap and go", Zelle, Venmo) opened additional avenues of risk through increased transaction speeds and the opportunity to steal payment information. Moreover, cryptocurrency has allowed for greater payment anonymity and is a widely unregulated space. These factors have made these payment types attractive to criminals. Financial institutions are faced with an increased exposure to fraud losses given the regulatory perspective on digital payment liability.

Internal pressures, heightened by the possibility of a recession, add to these challenges. Fraud risk management and Fraud operations are cost overheads, targeted at saving the financial institution from fraud losses. Technology in these programs do not typically receive increased investment or enhancements leaving legacy processes unchanged unless external pressures force the matter. As a recession looms, fraud teams across the industry will be expected to continue to minimize fraud losses while keeping operating costs low, potentially even reducing their overheads. The prospect of reducing the costs of operating a fraud program inherently increases fraud risk.

To be effective at managing fraud risk, Fraud operations teams need to be nimble and Fraud risk management teams need to have made investments in establishing an effective fraud risk management program. They need to be able to identify fraud surges and fraud attacks earlier and be better at discerning who is a bad actor and who is a true customer (and in recent years this has become more challenging). These teams need to be prepared to react, leveraging skilled **people**, efficient and effective **processes**, emerging **technology**, and timely and accurate **information**. But equally important is the culture around which these programs operate. Leadership needs to set a tone at the top, one that stresses the need for the institution to be "fraud ready". "Fraud Ready" means that an institution has the flexibility and processes in place to always be looking ahead for the next wave of fraud. Successful Fraud Ready institutions establish processes on how to react quickly to emerging threats and stand-up responses to these frauds without over governance and rules with a focus on rapid reaction for the protection of their customers and their own business lines.

So how can financial institutions be more proactive? Better yet, how can organizations build a culture that aims to mitigate risk and be "fraud ready?". KPMG's Financial Services Fraud professionals have a well-established track record of helping Fraud risk management leaders and operations teams to proactively get to this state. Ranked as #1 for Most Authoritative Risk Firm, Quality of Risk Transformation, and First Choice Risk Advisory Firm to Work With,[2] KPMG can assist our clients through:

- **Current state assessments and risk assessments** that help identify areas for process improvements, and furthermore formulate a transformation strategy that can help firms get to a "fraud ready" state efficiently;

[2] Source: Source Global, Perceptions of Risk Firms in 2022 (August 2022)

- **Strategy working sessions** that can help fraud leadership identify technology solutions that address top-of-mind challenges, help reduce redundancy, and formulate a roadmap to achieve an enhanced state;
- **Process simplification reviews, fraud technology implementations, and fraud rules tuning exercises**, that can improve the functionality of your existing program by reducing volumes and significantly reduce the cost of running those processes;
- The **outsourcing of fraud operational processes**, through a managed service model, either in whole or in part. Where KPMG has taken over an entire process, our clients have saved up to 50% while maintaining a 95%+ quality track record;
- **Fraud alert, and case surge support** that, arranged on an on-call basis, can help firms alleviate the pressure of fraud volumes when they increase;
- **Fraud investigations support** where KPMG professionals work alongside firm resources to investigate specific fraud schemes and assist in enhancing the controls implemented to mitigate identified schemes and others moving forward; and
- **Fraud training development and delivery** that help institutions train on the latest fraud best practices, industry insights and trends, allowing them to upskill their workforce and educate their customers.

Whether your institution is looking for assistance in enhancing a component of your Fraud program or wants to tackle the daunting task of overhauling your program to get to a "fraud ready" state, KPMG's Fraud professionals can support you every step of the way.

Contact us

Marc Miller
Partner, Global and US Forensic Leader
KPMG LLP
T: +212-872-6916
E: marcmiller@kpmg.com

Jennie Jonas
Managing Director, Forensic
KPMG LLP
T: +917-438-3563
E: jenniemorris@kpmg.com

Steven D'Antuono
Partner, Forensic
KPMG LLP
T: +202-533-3000
E: sdantuono@kpmg.com

Michaela Soctomah
Managing Director, Forensic
KPMG LLP
T: +617-988-5710
E: msoctomah@kpmg.com

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