COVID-19 implications: external fraud

Minds made for protecting financial services

Building a better working world

Introduction

The COVID-19 pandemic has heightened the risk of fraud due to an abrupt change in working practices, as well as increasing pressure on organizations, their customers and their supply chain. In addition, many governments have announced support packages for businesses using financial services institutions as a vector, which will open up new avenues for fraudsters.

This article focuses on the heightened external fraud risks associated with the COVID-19 crisis. These include:

- Increased pressure on banks to support customers who are affected by COVID-19, and fraudsters will attempt to take advantage of the funding and relief available from banks and governments. Insurers are likely to come under the same pressure once their policyholders start to make business interruption claims.
- Fraudsters are rapidly adjusting their approaches to take advantage of the crisis (for example, distributing malware or redirecting payments).
- The squeeze on revenues and incomes may increase the pressure on customers to commit first-party fraud (such as fraudulent loan applications). All finance and insurance requests and claims, even for the most long-standing customer relationships, should therefore be subject to additional scrutiny.
- Remote working and the greater use of less secure home networks increases fraud and cyber risks. In addition, enterprise-wide controls to prevent and detect fraud and network breaches may not be designed to operate in near-100% virtual environments.
- 'Action Fraud' is running a reduced service, which may limit industry collaboration and fraud intelligence sharing capabilities at a critical time.
- The Payment Systems Regulator has announced that it will not take any action against banks that delay the introduction of Confirmation of Payee (CoP) until 30 June 2020 – several months after it was due to be introduced. CoP is an important initiative to help reduce the number of scams, which may well increase as current self-isolation restrictions lead customers to be more vulnerable to this sort of fraud.

Ask us for other EY Financial Crime and Forensics COVID-19 implication papers:

- Bribery and corruption risks
- Internal fraud
- Market abuse
- Navigating the impacts of the pandemic on financial crime compliance
- The internal investigation process
- The whistle-blowing function

Source 1: https://www.transparency.org/news/feature/in_times_like_these_transparency_matters_more_than_ever.

Red flags: what to look out for right now

- As organizations rapidly onboard new third parties to help them respond to the crisis, there is a risk that usually robust onboarding, screening, procurement and payments controls are relaxed or overlooked to speed up onboarding and secure products or services.
- The US Financial Crimes Enforcement Network (FinCEN) has recently circulated guidance that identifies the risk of criminals and fraudsters attempting to solicit donations, steal personal information or distribute malware by impersonating government agencies (e.g., Centers for Disease Control and Prevention), international organizations (e.g., the World Health Organization) or other healthcare organizations.
- Organizations that use third-party intermediaries, such as brokers or distributors should rigorously review the activity of these intermediaries, particularly if they may be in financial distress and there is a variable element to their pay (e.g., the number of customers signed up or insurance policies written).
- We expect banks to see an increase in applications for credit cards and loans to help with cash flow during these challenging times. Banks should remain vigilant to heightened risks of application fraud from fraudsters, while they contend with higher than usual volumes of applications.
- Similarly, insurers may find customers inflating claims for recent but unrelated events, such as the widespread flooding in the UK, to obtain more funds to maintain cash flow.

Changes in customer spending habits are creating a higher number of false positives in organizations' transaction profiling systems: i.e., a reduction in face-to-face transactions and increased online shopping.

Unfortunately, there are some frauds, in areas such as trade finance, receivable financing and invoice financing, that are increasingly likely in the current environment, but have few red flags (such as one-off singular payments or rapid changes in customer behavior). Therefore, they are difficult to identify. Instead, more circumstantial evidence, such as a customer's willingness to 'bend the rules' with respect to tax or other legislation, and comparing their financial performance and funding requirements with that of their peers, is a useful proxy.

Scams and fraud against firms' customers

During these uncertain and unpredictable times, fraudsters will attempt to take advantage of the situation. As customers fall victim to fraud, they will look to their banks and insurers to cover their losses. Topical fraud includes:

- **Charities fraud:** fraudulent charities target victims for donations. Such schemes can originate from social media, emails, websites, mailings, telephone calls and other similar methods.
- **Cyber fraud:** malicious cyber actors will attempt to take advantage of public interest in topical news, such as local infection rates or changes to public services, to disseminate malware.
- **Invoice redirection fraud:** businesses and commercial banking customers will be at increased risk as their operations adjust to cope with the impact of COVID-19 (for example, finance teams working remotely may be more susceptible to invoice redirection fraud). We have heard of several cases of this type of fraud involving global banks whose customers have lost more than £5m.

What does this mean for you?

Immediate actions

Personnel changes

- Focus on educating employees on the increased risks from fraudsters seeking to capitalize on the current disruption.
- Consider combatting the heightened fraud risk by moving personnel, especially financial crime data analysts, from other parts of the organization to respond to the higher number of fraud alerts. Fraud teams are also redeploying resources internally to respond to the changes in the volume of fraud alerts, as the mix of transaction types generating those alerts changes.

Profiling and identification

- Evaluate introducing facial or voice biometrics as part of the customer identification process. A number of organizations were introducing this prior to the pandemic. This may need to be expanded to other products and services as the crisis continues.
- Tailor fraud profiling systems to ensure they appropriately monitor customers' new behavior patterns. Systems should focus on known data points such as customers' phone numbers and IP addresses. Organizations should also increase their reliance on two-factor authentication.

Fraud typologies and risk categorization

- Consider phishing as a higher fraud risk route and use lessons learned from past attacks. The National Fraud Intelligence Bureau reported that it has received multiple reports about COVID-19-themed phishing emails, attempting to trick people into opening malicious attachments or revealing sensitive personal and financial information.
- Re-evaluate your customer risk strategies. Some categories of customers, such as non-profit organizations, charities, and healthcare and medical device manufacturers, may be considered as higher-risk categories, especially now, as they could become the conduits through which fraudsters attempt to penetrate financial systems.
- Closely monitor fraud losses and emerging fraud typologies. This can be achieved by fine-tuning the thresholds in fraud detection systems and focusing on identifying new fraud typologies. Monitor bad debt write-offs, which will likely include first-party fraud losses.

Customer support

- Remain focused on protecting customers from scams. This may include tailoring warning messages during the payment journey, tweaking payment risk scoring based on emerging scams or adjusting the thresholds required for manual review of higher-risk payments.
- Continue to look at ways to prioritize the process for obtaining customer recoveries for large scam losses. This process may quickly come under strain, with key employees working remotely or falling ill and receiving banks operating under similar constraints.

After the crisis has settled

- A review of major new contracts issued, and transactions and payments made over the crisis period, should be undertaken, to understand if any risk mitigation and management is required. Consider leveraging technology to make these processes easier – e.g., analytics to review high-volume, lower-value transactions such as gifts and entertainment, or payments to third parties to identify outliers during this period. This also applies to any insurance claims stemming from events during the crisis period.
- A review of vulnerabilities that have arisen from the crisis-specific controls that were not adequately designed or not operating effectively or efficiently should be undertaken. Consider whether any controls that were revealed to be redundant could be streamlined.
- Organizations should confirm that whistle-blowing channels and supporting infrastructure are still available to employees and third parties to report any inappropriate behavior identified during the COVID-19 crisis. Even if there is no immediate capability or capacity to investigate, once the dust has settled, a review of matters reported can be undertaken.

Vulnerable and higher-risk customers

Vulnerable customers are at heightened risk of falling victim to scams for several reasons, including:

- They may not be very tech savvy but, now, may only be able to interact with their financial service providers online.
- Anxiety about themselves and loved ones' health, or loneliness due to social distancing and isolation, may make them more welcoming of conversation from strangers than usual.

Increasing the population of those who would typically be considered vulnerable is something organizations may have to do: for example, those who are at heightened risk from COVID-19 (such as pregnant women or young people with underlying health conditions) may not have been identified as vulnerable customers before. However, the requirement to self-isolate, and the accompanying mental duress that it may place on them, may make them more susceptible to scams.

Organizations should also recognize the vulnerability of other customers to these scams: for example those who have lost their jobs may be susceptible to 'get rich quick' investment scams, or be at risk of being targeted by organized crime gangs to become money mules.

Key contacts

For further information, please contact the Financial Crime and Forensics team.

Rachel Sexton
Partner, Ernst & Young LLP
+44 20 7951 1179
rsexton1@uk.ey.com

David Higginson
Partner, Ernst & Young LLP
+44 779 877 4840
dhigginson@uk.ey.com

Glenn Perachio
Partner, Ernst & Young LLP
+44 20 7951 4628
gperachio@uk.ey.com

Julie Fenton
Partner, EY Business Advisory Services
+353 86 383 5556
julie.fenton@ie.ey.com

John Clinton
Associate Partner, EY Business Advisory Services
+353 87 231 5205
john.clinton@ie.ey.com

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.
EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

© 2020 EYGM Limited. All Rights Reserved. EYG no. 002424-20Gbl ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.