2020

Fraud and Economic Crime – opportunity in the face of adversity

PwC Kenya Economic Crime and Fraud Survey

www.pwc.com/ke

pwc

The news and topics that have been pervasive in the airwaves and social media lately are depressingly familiar and concern theft and loss of resources. The amounts being discussed are also becoming larger with each newscast. Cases of inflated contracts, fraudulent and corrupt deals and collusion in many of the organisations as business and organisations count their losses as they reel from the economic crimes. The news make for depressing reading and point to a vicious cycle and a race to the bottom.

As per the GDP growth indicators released by the World Bank[1], the Kenyan economy grew by 5.7% in 2019 and is further projected to grow by about 6% in 2020. Despite this reported growth, many businesses have had to tighten their belts to ride out what has been a challenging business environment. The Government is also facing a tough task balancing its books as the economic belts tighten further and the gap between revenue targets and collections widen.

Within the last two years covered by this survey, the rate capping law that was introduced in late 2016 was in place for most of the period, having only been abolished in November 2019. The squeeze on credit in the period it was in effect saw small and medium size businesses struggle to access financing thereby hindering their respective growth agenda.

In the same period, the Central Bank of Kenya replaced the 1,000 shilling note in an attempt to fight corruption and illicit flow of money in the economy. The efforts to counter laundering of proceeds of crime in the financial sector also saw the Central Bank of Kenya enforcing relevant provisions of the Proceeds of Crime and Anti-Money Laundering Act ("POCAMLA") and regulations and demanding financial institutions to demonstrate that their compliance programmes are adequate and effective. The KRA has also cranked up efforts to ensure tax compliance through concerted pursuit measures against tax cheats.

The Government also enhanced its efforts in the fight against corruption with high profile arrests being made by the DCI and numerous graft cases being brought to the courts. A number of impeachment cases on account of alleged graft have also been brought against high profile politicians.

Despite these efforts, a number of questions remain relevant: are we doing enough? Are we matching up to economic criminals as they innovate and up their game? Are we prepared to not only embrace the increasingly sophisticated technology designed to deliver the much desired efficiencies and great customer experience but also deal with the tech-enabled economic crime threats?

Our Survey this year seeks to provide some insights into these questions as well as assess the extent to which the effective management of economic crime is having a positive impact on Kenyan organisations.

[1]https://www.worldbank.org/en/country/kenya/overview

Economic crime

For over 20 years PwC's Global Economic Crime and Fraud Survey has looked at a number of crimes, including:

- Accounting/Financial Statement Fraud
- Anti-Competition/ Antitrust Law Infringement
- Asset Misappropriation
- Bribery and Corruption
- Customer Fraud
- Cybercrime
- Deceptive business practice
- Human Resources Fraud
- Insider/Unauthorised Trading
- Intellectual Property (IP) Theft IP
- Money Laundering and Sanctions
- Procurement Fraud
- Tax Fraud

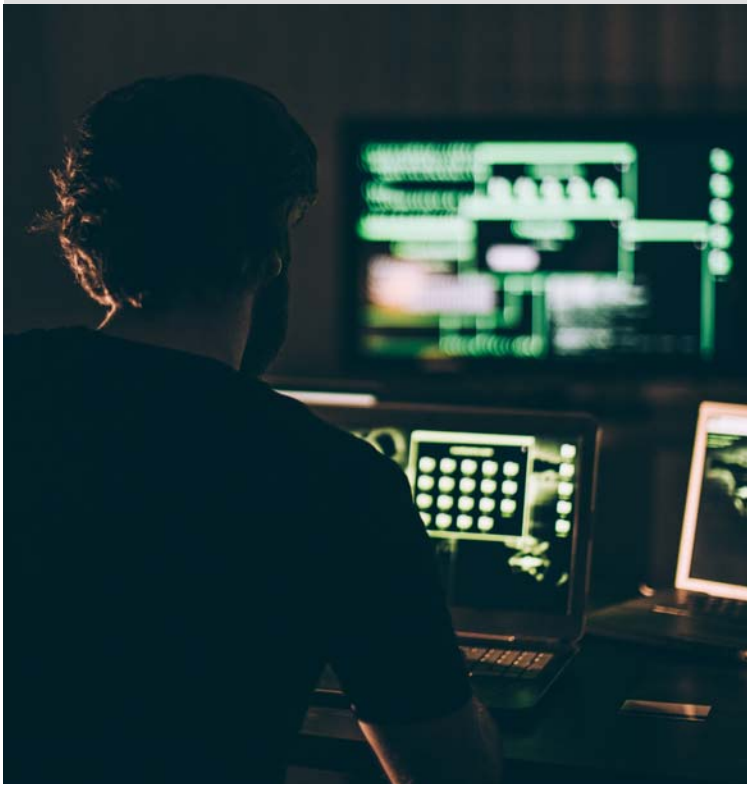
By the numbers –

Our survey findings

When Fraud Strikes: **Incidents Of Fraud**

2020 saw a decrease in the reported incidents of fraud over the 24 month survey period.

In this Report, we share insights on the types of economic crimes being perpetrated, who is committing the crimes, attitudes towards economic crimes and the steps successful organisations are taking to combat the vice.



5,000+

respondents globally, with 102 drawn from Kenya

62% of the respondents from organisations with US$ 10m+ in global revenues

99

territories globally participated in the survey

Ksh5.5b

was lost by Kenyan respondents

58%

of Kenyan respondents told us they **experienced economic crimes in** the past two years, down from **75%** in 2018, but still higher than the Global average of **47%**

44%

of Kenyan companies that experienced economic crimes had between **6-10 incidents** reported in the last 24 months

Top 4 types of fraud

1. Bribery & Corruption
2. Procurement fraud
3. Asset misappropriation
4. Customer fraud

The reported incidences of Procurement fraud in Kenya is more than double the global average and Procurement fraud was also noted to be the most disruptive. Globally, Customer fraud and Cybercrime led the pack.

Types of Economic Crimes experienced

Source: PwC's 2020 Global Economic Crime and Fraud Survey

Most disruptive Fraud events

	1	2	3
Kenya	Procurement Fraud 15%	Bribery and Corruption 14%	Accounting/ Financial statement fraud 14%
Africa	Bribery and Corruption 17%	Accounting/ Financial statement fraud 15%	Customer fraud 15%
Global	Customer fraud 16%	Cybercrime 16%	Accounting/ Financial statement fraud 14%

Procurement fraud and Bribery & Corruption, have a correlation in our part of the globe, with various cases of rent seekers in procurement deals seeking to profit illicitly by asking for facilitation fees or kickbacks.

Incidentally, about a third of the respondents reported having been asked to pay a bribe in the past 24 months.

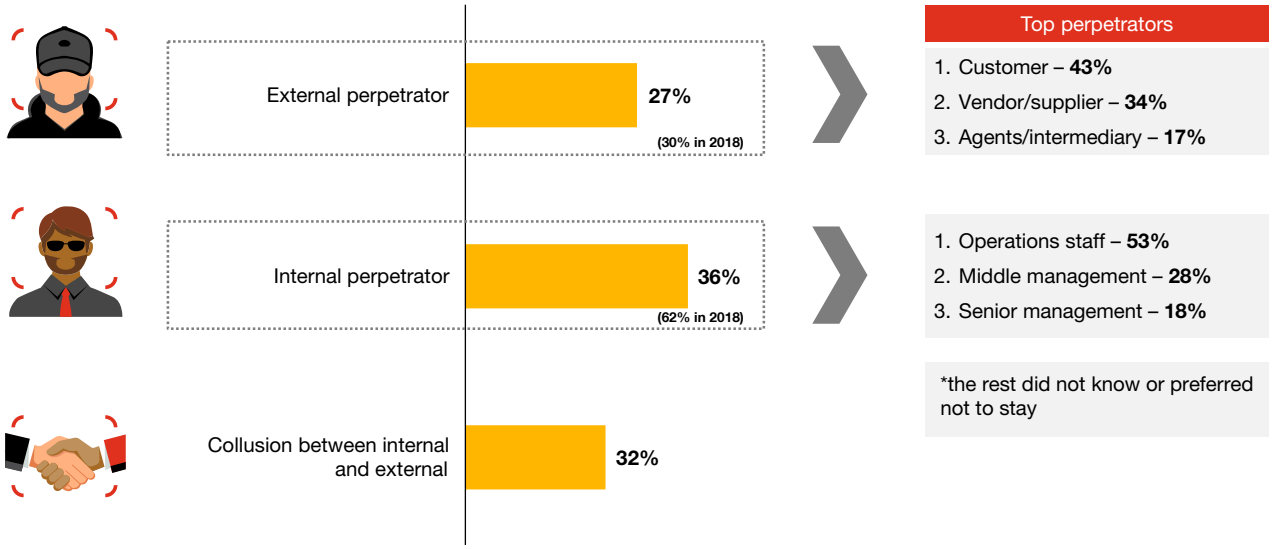
Source: PwC's 2020 Global Economic Crime and Fraud Survey

The Perpetrators: **Who is committing these crimes?**

Organizations face multiple threats in terms of where the next economic crime attack would originate. It could be internal; from the Board, management, operations staff; it could also be external; your customers, organized crime syndicates, suppliers; or a joint effort where both internal and external parties collude.

In the past, most of the incidents were perpetrated internally, however in most cases there is an element of collusion with external actors.

In Kenya and in Africa, internal parties were reported to have been the most common perpetrators of economic crime unlike globally where the incidents by external perpetrators were higher.



Source: PwC's 2020 Global Economic Crime and Fraud Survey

Operations staff: Fraud committed by operations staff was the highest of the fraud attributed to internal actors at 53%. It could be an indication of the ineffectiveness of controls at lower levels or more daring attempts by junior staff. Middle level management were the most active group of internal actors in 2018 (decreased from 41% to 28%). Kenya, however, seems to be the exception, as elsewhere, senior management were reported to have committed more fraud.

Customer fraud: Customer Fraud continues to be rampant topping the list of external perpetrators of economic crimes at 43% of externally perpetrated economic crimes. Instructively, whereas Customer Fraud is the most prevalent globally at 35%, it is lower in Kenya where the prevalence rate is 32%.

Vendors and suppliers: As more companies invite vendors and other third parties into their organisations' operating environments through outsourcing of various services, they expose themselves to risks from parties seeking to illicitly enrich themselves at their expense. With 34% of economic crimes attributed to these third parties, this paints a scary picture as to the level of trust needed and risks organisations face in the business environments they are forced to operate in.

Accused of fraud? In a new question, we sought to find out if the respondents' organisations had been accused of perpetrating economic crimes. 18% of the respondents (and 15% globally) reported having been accused of economic crimes.

From the global survey results:

- In almost equal numbers, competitors, regulators, employees, and customers were most likely to point the finger.
- Enhanced regulatory focus, and in some territories, whistleblower incentives may contribute to this trend.

Cumulatively, the cost of economic crimes can be devastating.

In addition to the direct financial losses, organizations are exposed to fines and penalties by regulators, claims from affected third parties and damage to their brand and reputation, as well as dampening of employee morale, especially collateral victims not involved in the crimes.

36%
of Kenyan respondents that experienced economic crimes lost over
KShs 10million

with 2% reporting losing in excess of KShs 500million

Some economic crimes such as Money Laundering, Bribery & Corruption, can have untold consequences, as some of these crimes are subject to laws in multiple jurisdictions.

This is especially so for multinational organisations listed in the US and UK stock exchanges where Bribery and Anti-Corruption laws transcend borders. Fines from regulators can cripple organisations found on the wrong side of these laws.

Six costliest frauds in Kenya

1	Procurement Fraud	15%
2	Bribery & Corruption	14%
3	Accounting/ Financial Statement fraud	14%
4	Asset Misappropriation	12%
5	Customer fraud	12%
6	Money laundering & sanctions	12%

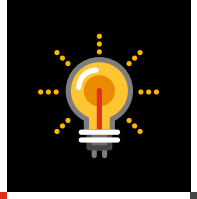
Diving In

Bribery and Corruption remain a big challenge not just in Kenya. A third of respondents both globally and in Kenya reported being asked to pay a bribe or had lost an opportunity to a competitor who they believe paid a bribe.

39% of respondents reported experiencing **Procurement fraud,** which was significantly higher than the global average of 19%. Ranked as the second most prevalent form of economic crime in Kenya, it was also the costliest and most disruptive type of economic crime experienced by Kenyan respondents.

It is encouraging to note the level of awareness and response to the risk, with 70% of the Kenyan respondents putting in place programmes in their organisations to deal with Bribery & Corruption, higher than the global average of 39%. 56% of the Kenyan respondents also reported having a dedicated programme to address the risk of Procurement fraud, a figure that is also more than twice the global average.

Combating economic crimes



Taking action: **Being prepared**

Combating economic crime is usually a continuous process that adapts and changes to match the innovative nature of fraudsters.

It is sometimes argued that some of the most creative research and development ideas originate from fraudsters, who come up with novel ways to beat controls and safeguards.

What is your organization investing in to stay ahead of the fraudsters?

More than half of the organisations have documented risk-based due diligence and ongoing monitoring processes for third parties as well as dedicated programmes to address Bribery & Corruption, Accounting/ Financial statement fraud, employee fraud and Procurement/ vendor fraud.

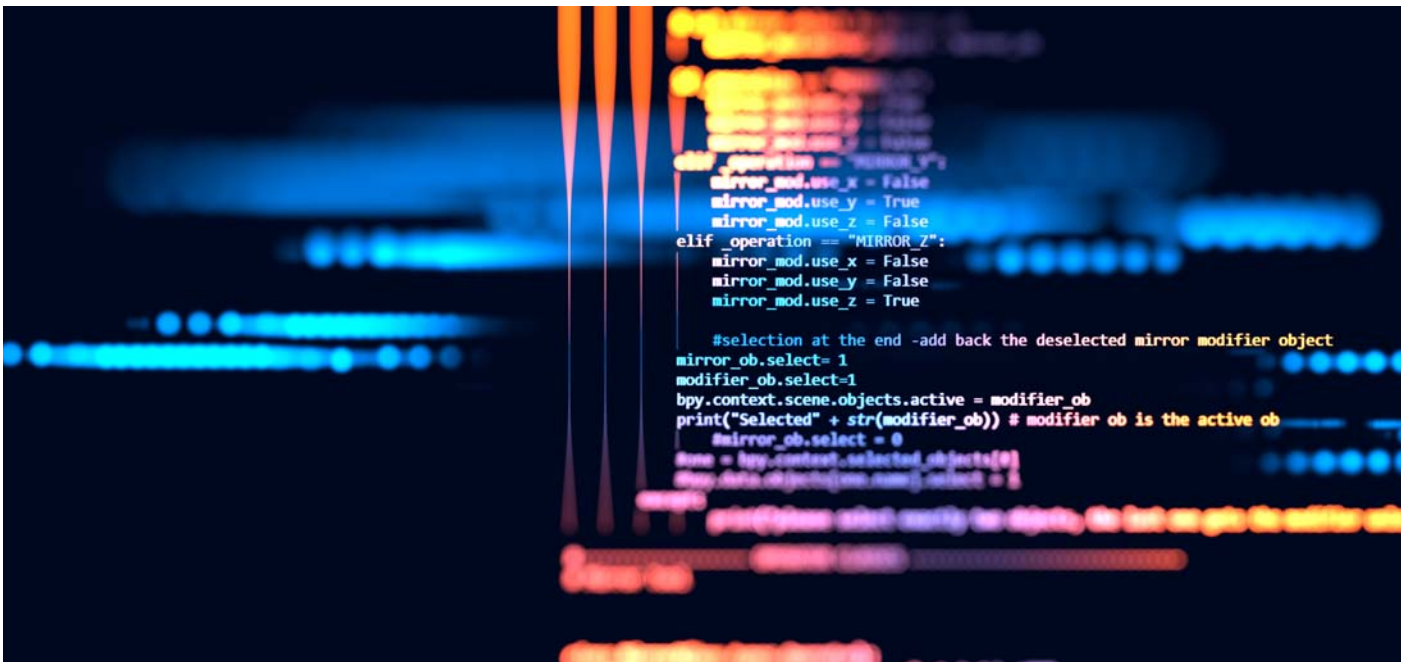
We further found that:

- 4 out 10 respondents either don't perform or perform only informal risk-based due diligence and ongoing monitoring of third parties.
- 84% of respondents have formal documented policies and procedures and controls for key compliance areas, more than the global average of 64%.
- A third of the organisations perform limited testing of the effectiveness of the controls with 5% not carrying out any tests.

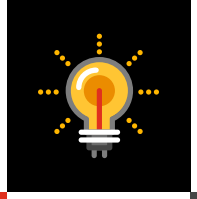
84% of respondents have formal documented policies and procedures and controls for key compliance areas, more than the global average of 64%

What are the most effective actions?

1. **Robust risk assessments.** Obtaining input from both internal and external stakeholders and continuously updating the approach of carrying out the assessments as risks are dynamic and fraudsters are highly adaptable.
2. **In addition to employing technology, investing in the right expertise, governance structures and monitoring mechanisms.** Advanced technology by itself is not sufficient to combat economic crimes.
3. **Reaction time.** Deploying the right tools and personnel to investigate and address a potential economic crime is critical. It enhances controls by deterring fraudsters in the first place.



Rise of technology



Taking action: **Keeping up**

As organisations strive to be more efficient and better serve an ever-growing client base, they continuously adopt more complex technology. As this happens, attacks aimed at the systems or designed to utilize these systems also become more sophisticated in scale and methodology. As such, organisations have no option but to invest in ever more complex anti-fraud technology.

This unfortunately increases the risk of the technology employed being ineffective especially where knowledge of how such technology works is limited to a few individuals in the organisation. There is also a risk that organizations will erroneously assume that the technology they have invested in, since advanced, can in isolation of other measures, protect them from fraud.

We asked our respondents what alternative/disruptive technologies/techniques they have invested in and whether they find value in it helping combat fraud and other economic crimes and found that:

Technology	% Currently using and finding value
Communications Monitoring	57%
Transaction Testing / Monitoring	55%
GRC (Governance Risk and Compliance) Solutions	47%
Anomaly Detection	41%
Contract or Other Unstructured Data Review	35%
Data Visualisation / Dashboards	35%
Pattern Recognition	29%
Predictive Analytics	23%
Artificial Intelligence (AI)	14%

Although AI ranked lowest, it is widely seen as the future in crime busting technology. This is due to its ability to harness big data and ability to augment the other technologies and more traditional methods of combating economic crimes.

Of the common AI technologies that also include Natural Language Processing (NLP), Natural Language Generation (NLG), Voice Recognition and Machine Learning; Kenyan respondents highlighted Biometric Authentication as the most widely and beneficial AI technology with 34% of Kenyan respondents installing and deriving value from it.

Biometric technology has been refined over the past few years with deployment of fingerprint readers and facial recognition software improving tremendously. Smart phone developers have been key in fast tracking the development and widespread use of this technology.

According to our respondents, cost, limited resources to run/handle results and lack of (appropriate) systems were the top three reasons preventing their organisation from implementing / upgrading technology in order to combat fraud, corruption or other economic crimes.

Technology is dynamic, changing every so often with new ones coming up every year. Who knows what novel technologies we shall be discussing in 2 years' time as the dance between economic criminals and organisations continues.

Our attitudes towards fraud

78% of Kenyan respondents that reported having suffered an economic crime conducted an investigation.

This is commendable as it is important to establish the facts around an incident to enable you improve your control environment to prevent recurrence of similar incidents in future.

However, only 27% disclosed the matter to regulators/ law enforcement, with the majority choosing to keep and deal with the matter in-house. Should we be worried about the confidence our organizations have in our regulators and law enforcement agencies?

Organisations adopted the following key steps to better themselves as they reacted to incidents of economic crimes:

1. Conduct an investigation – 78% - To get to the root cause of the crime and establish the facts.

2. Disciplined/ Terminated employees - 63% - Subject to labour laws and disciplinary and other related policies within organisations.
3. Implemented enhanced internal controls – 61% - Enhancing the controls in place to make it more difficult for criminals targeting the organisation.

In Africa, cyber crime ranks amongst the top areas of concern with 38% of CEOs citing it as a threat

Only
31%
of Kenyan respondents **conducted training** to staff following an incident

Training does not only better inform staff of new policies and procedures, it also promotes a stronger culture around fighting fraud and it is commendable how Kenyan organisations are keen to raise awareness.

Source: PwC's 2020 Global Economic Crime and Fraud Survey

78%

of respondents who experienced some form of **economic crime in the last 2 years** believe that despite the negative consequences, their organization is in a better place as result of the experience

Source: PwC's 2020 Global Economic Crime and Fraud Survey

Taking stock

Everyone would want to avoid falling victim to an economic crime, and whether it is by luck or being prepared, the best outcome most would prefer is sailing through unnoticed and unscathed by criminals.

The monetary loss, time and resources spent in dealing with economic crimes can be significant. However, as observed in the survey, it can result in a turn for the good, an awakening call and change of attitude towards fraud risk and potentially a transformation of the organisation's operations.

74% noted an enhanced tone at the top and control environment in addressing economic crimes following an incident, with 67% experiencing streamlined and improved operations as well as fewer repeats of the incidents.

20% of the organisations noted improvement in employee morale and there was a noted impact in financial performance with 28% seeing a reduction in losses of which 9% saw improvements in revenues and profitability.

On the flipside, 33% suffered damaged brand trust and reputation, 34% noted a decrease in revenues and profitability and 29% saw an increase in losses and lowered employee morale.

Depending on how the organisation prepared itself, it can come out more resilient at the end of the crisis or, in a more extreme case, or cease to exist altogether.

Almost 92% said they experienced negative emotions after an incident of fraud

The most common feelings were **frustration and anger**

33%
suffered damaged brand trust and reputation

Source: PwC's 2020 Global Economic Crime and Fraud Survey

Given the ever present and evolving threat of economic crime that keeps organisation leaders awake and alert, as well as other business issues that compete for attention and resources from management, how do business leaders navigate and address the fraud risks at the same time?

Quantifying the benefits and successes of an elaborate fraud fighting system is not easy. In some cases, it is akin to proving a negative, which in itself is an arduous task. That is why in some organisations, the default attitude is to only invest in combating economic crimes where they have fallen victim in the past or where there are mandatory regulatory requirements to have measures put in place. Investment in proactive fraud fighting tools and resources are for such organisations not a priority.

It can be challenging to quantify the benefits of a fraud-fighting tool. Effective fraud prevention measures do reduce the quantity and magnitude of future fraud. But here's a more interesting statistic – there is a clear link between fraud prevention investments made upfront and reduced cost when a fraud strikes.

From the manner in which the economic crimes were detected:

12% through suspicious activity monitoring

10% through routine internal audits

10% through tip-offs

8% through Fraud risk management

the benefits of having proactive monitoring processes and whistleblowing hotlines in place are evident.

Source: PwC's 2020 Global Economic Crime and Fraud Survey

Once you have a programme in place, periodic assessment and refinement is key. Why?

- From our global survey, we note that business models frequently evolve before risk programmes are established, leaving companies exposed to unexpected risks.
- There's increasing convergence in certain industries that is heavily driven by data — In Kenya, Telcos offer financial services, banks are offering insurance services, health companies are entering consumer markets, etc — risk management programmes need to be adapted to meet those new or evolving opportunities and risks.

- Information that is unexpected from the controls in place, such as a hotline call, whistleblowing email or an audit finding may yield a risk previously not considered.

Where companies are slow to implement measures to mitigate economic crimes, regulators are moving in to give the organisations a nudge to improve surveillance and compliance programmes.

In the East African region, especially in the Financial Services Sector, we have observed the regulators directing companies to provide evidence of compliance programmes and regular independent reviews.

The benefits from these initiatives may not be immediately visible as they may take a bit of time for the effects to be noticed.

In the East African region, especially in the Financial Services Sector, we have observed the regulators directing companies to provide evidence of compliance programmes and regular independent reviews

Some of the initiatives, e.g. training or third party management programmes may also not be easy to quantify, and this while providing organisations with a challenge justifying the initiatives, also provides them with an opportunity to be trailblazers to set their key metrics to measure the effectiveness of these initiatives.

In conclusion

How would you gauge your personal or organisation's preparedness in combating economic crimes? What are your attitudes towards economic crimes?

Does it affect you or do you consider it someone else's problem?

Awareness is key prior to setting out on any program to address fraud and other economic crimes. Identifying the risks, keeping up with technology and regulatory advancements arms you with the requisite knowledge to devise controls and initiatives to mitigate the risks.

In the event you fall victim, it is also useful to be prepared with a well thought out response mechanism and system.

Economic crimes are dynamic and unpredictable, and the only way to minimize the risk is preparedness and adaptability.

Finally, if well prepared you may very well emerge from an incident of economic crime stronger and better prepared to avoid future recurrence.

Contact us

At PwC, we carry out fraud risk assessments and cyber security assessments to help you identify key risks and threats. Our assessment teams are fast and cost-effective, combining global leading best practices and in-market experience. In addition, we provide investigation services to detect economic crime. Our regional team of dedicated specialists has conducted some of the most complex and high profile investigations undertaken in Kenya and regionally in recent years.

Muniu Thoithi
Advisory & Forensics Leader,
Eastern Africa

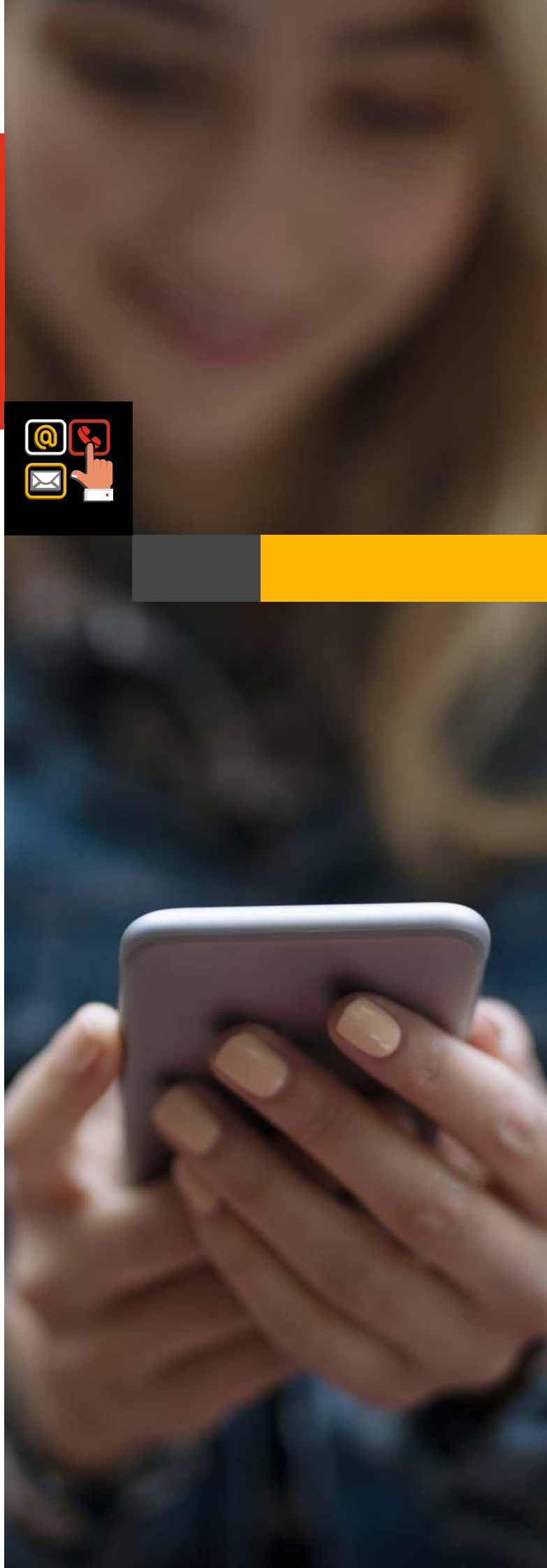
muniu.thoithi@pwc.com
+254 20 285 5684

John Kamau
Associate Director,
Forensic Services

john.kamau@pwc.com
+254 20 285 5065

Eric Owino
Senior Manager,
Forensic Services

eric.owino@pwc.com
+254 20 285 5692



At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2020 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.

Please see www.pwc.com/structure for further details