Meeting tomorrow's challenges, embracing risk intelligently

PwC's Global Economic Crimes Survey 2024: Uganda Report

pwc

Foreword

The 2024 Global Economic Crimes Survey (GECS) covers the immediate last two years after the Covid-19 pandemic subsided. This period was characterised by adaptation and normalisation of new ways of doing things. The new normal includes adoption of hybrid working models that combine both remote and in-person collaboration; optimization of supply chains; adaptation of consumer preferences such as omnichannel strategies; and refinement of new digital, business resilience and risk management strategies.

The economic crime environment appears to have evolved with the shift in operational practices from the pre-pandemic era, through the pandemic to the post-pandemic era underscoring the need to continuously update risk management practices and strategies.

For instance, the cybercrime incident rate that ranked a distant eight (8) in the GECS 2020 Uganda report (covering the pre-pandemic years of 2018 and 2019) has now leap-frogged other forms of surveyed economic crimes to rank a close number two (2) behind customer fraud. Globally, **cybercrime is now reported as the most prevalent form of economic crime** at an incident rate of 44% and as the **most disruptive by 40%** of the respondents.

Similarly, the PwC Eastern Africa 2024 CEO Survey cites cybercrime as an increasing area of concern with 28% of CEOs citing it as a threat up from 22% in 2023. The Eastern Africa CEOs also cite macroeconomic volatility as the top area of concern in the next 12 months. Macroeconomic volatilities come with market uncertainties, financial pressures and incentives which are fertile grounds for convergence of the elements of the fraud triangle. Counter-fraud practitioners and risk management functions should therefore sharpen their tool kits for potential headwinds ahead.

63% of respondents in Uganda reported experiencing fraud or another form of economic crime in the last 24 months. This is a marked increase from 54% in the 2020 report and higher than the Eastern Africa and Global averages of 48% and 41% respectively. The Uganda trajectory is contrary to the Eastern Africa and Global incident rates that have improved from 59% and 47% respectively in 2020.

Not all is gloom and doom. Globally, most organisations report as having adopted fraud risk management programs and are increasingly leveraging data analytics and technology to manage fraud risks. In Uganda, **64% respondents reported having undertaken an enterprise-wide fraud risk assessment in the last 12 months and 27% reported using data analytics and technology** for compliance monitoring and to provide insights to improve programme effectiveness. Further, 52% project that new technologies and systems such as artificial intelligence (including machine learning and generative AI) will dramatically increase the efficiencies of their compliance programmes including reducing costs. We expect the benefits of these to be reflected going forward in increased awareness, detection, and deterrence.

GECS 2024 survey findings: An overview

The 2024 survey attracted 2,446 respondents from 77 countries drawing responses from top management including Board members, C-suite executives, Risk & Compliance as well as internal audit professionals.

77 Countries Globally

Global survey of 2,446 respondents across 77 countries with 59 drawn from Uganda

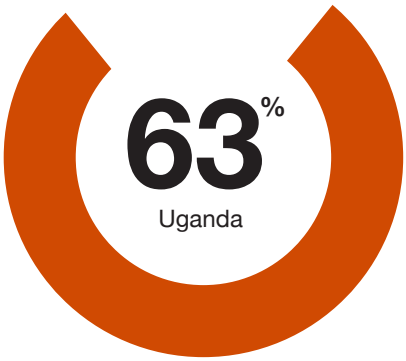
7 Countries in Eastern Africa

256 surveys were completed within Eastern Africa with Uganda accounting for 59 of the respondents

74% of the Uganda respondents were either C-suite executives or Board members with the rest drawn from risk, compliance and internal audit functions. These were drawn from diverse sectors with 63% of the respondents drawn from the financial services sector including banking and capital markets, insurance, asset, and wealth management.

- Financial services, 63%
- Industrial & Manufacturing, 14%
- Government & Public Sector, 11%
- Technology, Media and Telecom, 9%
- Health services, 4%

63% of respondents in Uganda reported experiencing fraud or another form of economic crime in the 24 months covered by the survey. This is a marked increase from 54% in the 2020 report and higher than the Eastern Africa and Global averages at 48% and 41% respectively in the current survey.



48% Eastern Africa

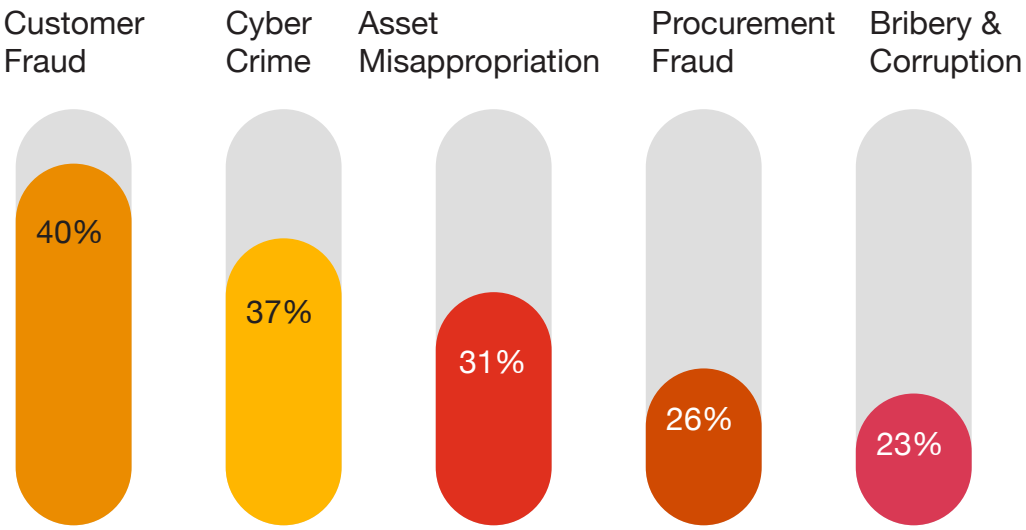
41% Global

63% of respondents from Uganda reported experiencing economic crime in the last 24 months compared to an incident rate of 48% in Eastern Africa and 41% globally.

GECS 2024 survey findings: An overview

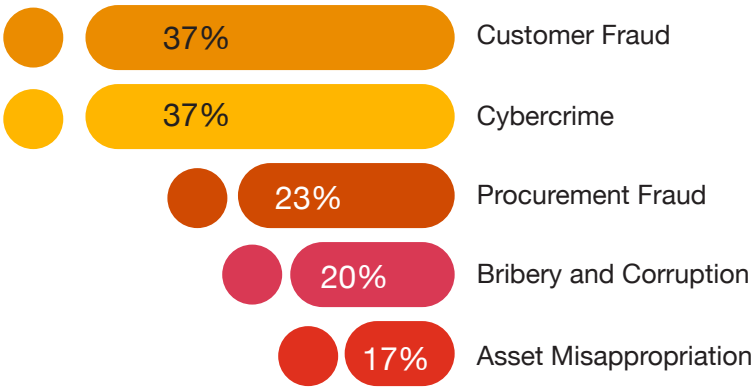
Customer fraud was reported as the most experienced form of economic crime in Uganda with an incident rate of 40% followed closely by cybercrime at an incident rate of 37%. Adoption of technology might have fuelled the shift in the nature of experienced economic crimes with a rise in cybercrime incidents while traditional forms such as asset misappropriation and procurement fraud have fallen down the pecking order with time.

Most experienced forms of economic crimes



Customer fraud and cybercrime were rated as the most disruptive forms of economic crime by 37% of the respondents. This is with respect to monetary loss or otherwise including operational interruptions, damage to reputation, and loss of trust.

Forms of economic crimes reported as most disruptive



While asset misappropriation was reported as the third most prevalent form of economic crime at an incident rate of 31%, the respondents assessed it as less disruptive as compared to the other reported forms of economic crimes. The closely related procurement fraud and bribery and corruption were assessed as more disruptive, behind customer fraud and cybercrime. This could be due to the fact that some of the most common asset misappropriation schemes such as inventory pilferage, cash larceny, expense reimbursements and misuse of organisational assets like vehicles often involve lower value transactions – overtime, these could however cause significant losses.

While increased technology adoption appears to have provided an opportunity for evolution in the nature and complexity of economic crimes, organisations are increasingly leveraging data analytics and technology in their risk management processes:

64% of Uganda respondents reported having undertaken an enterprise-wide fraud risk assessment in the last 12 months.

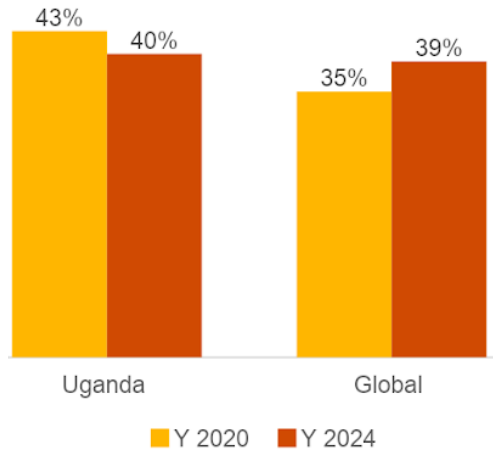
29% reported having used data analytics to identify unusual patterns for fraud mitigation which is a significant increase from the 2020 survey where only 14% of the respondents had used data analytics as an alternative technology/technique in combatting fraud and other economic crimes.

41% reported that government efforts to enforce anti-corruption laws have not improved in the last 12 months.

A deep dive into the economic crimes cited as most disruptive

Customer Fraud

Customer fraud involves fraudsters posing as customers to deceive businesses. This can be executed by both external perpetrators such as through identity theft or SIM swaps for mobile money account takeover schemes and by internal perpetrators such as through manipulating customer accounts or creating fake customer profiles. There are also cases of collusion where an insider provides sensitive information to an external perpetrator.



While the incident rate of customer fraud is reported to have reduced marginally in Uganda between 2020 and now, it has **increased at the global level** by four (4) percentage points signifying that **customer fraud will remain a significant threat in the future.**

Indeed 37% of the respondents assessed customer fraud, jointly with cybercrime as the most disruptive economic crimes in Uganda.

That customer fraud is paired alongside cybercrime as the most disruptive forms of economic crime in Uganda is no surprise. Many forms of customer fraud such as those cited above including payment fraud, identity theft, and account takeovers, leverage cybercrime techniques.

Observations from case studies in the region

We have in the recent past supported various players in the region to respond to concerns involving use of customer channels to defraud the respective organisations. It is important to note that fraudsters could combine multiple tactics in a single case to evade existing controls and/ or to cover up the fraudulent transactions. We highlight below some of the recent reported customer fraud cases:

a. One of the most reported schemes is account take-over of traditional bank accounts and mobile money accounts where fraudsters use social engineering tactics to trick users into revealing their personal identification number (“PINs”) or other sensitive information to gain unauthorised access to customer accounts. One of the landmark cases prosecuted in court (Atiku v Centenary Rural Development Bank Limited (Civil Suit 754 of 2020) 18 July 2022) involved an account holder losing UGX 55M (USD 15K) from their savings account through unauthorised transactions. Unlike some of the previous cases where banks were found liable, the Uganda High Court found the account holder liable for the loss in this case.

b. In a case that we helped investigate and that involved a manufacturing company, a senior staff member utilised privileged access to the organisation’s Enterprise Resource Planning (ERP) platform to allow fraudulent product uplifts by a customer disguised as credit sales. The scheme included irregular revision of credit limits in the ERP and posting of fraudulent credits in the customer’s account with the corresponding debits (s) touching unrelated accounts such as expense accounts. The senior staff member was also in charge of a number of other control activities which allowed perpetration of the scheme for an extended period of time. The exposure in this case totalled USD 2M.

c. Similar to the above case, we have also come across cases of use of post-dated cheques to allow irregular uplift of products without paying due consideration, credit fraud in trade finance instruments, and misuse of rebate systems, refund processes and sales promotions to extend undue credits to conflicted customers, sometimes at the expense of genuine and deserving customers.

Globally, the incident rate of customer fraud is highest in the financial services sector followed closely by the consumer markets sector covering retail, Fast-Moving Consumer Goods ("FMCG"), hospitality and leisure, and transport and logistics. This might explain the high incident rate in Uganda as most of its respondents were drawn from the financial services sector.

61% - Financial Services

45% - Consumer Markets

38% - Technology, Media and Telecom

30% - Government & Public Sector

29% - Health services

21% - Industrial & Manufacturing

18% - Energy, Utilities & Resources

Insights from other relevant publications/ statistics

Consistent with the above, the Bank of Uganda ("BoU") 2022/23 annual report[1] indicated that the number of customer complaints requiring compensation had doubled in the reporting period to stand at 2,346 complaints. The report did not provide a value of the complaints.

A consumer protection survey of digital finance users in Uganda by Innovations for Poverty Action (IPA)[2], an international non-governmental organisation raised concern of **low reporting of customer fraud incidents in Uganda citing lack of proper redress channels or non-responsiveness to complaints.** 47% of respondents reported to have experienced attempted scams or instances of attempted fraud with only 40% of customers experiencing financial loss who complained had their issue resolved.

Where to from here?

Call for constant vigilance and willingness to adapt

There is need to employ a multi-faceted approach to protect financial assets and customer trust. The response should include customer education, adequate KYC procedures, robust fraud prevention measures including adequate segregation of duties in key processes, detection systems, security protocols and staff training.

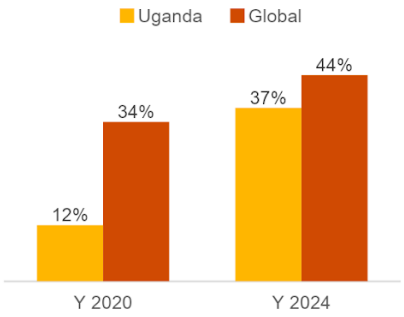
[1]Bank of Uganda 2022/23 annual report

[2]Consumer protection survey of digital finance users in Uganda by Innovations for Poverty Action (IPA)

Cybercrime

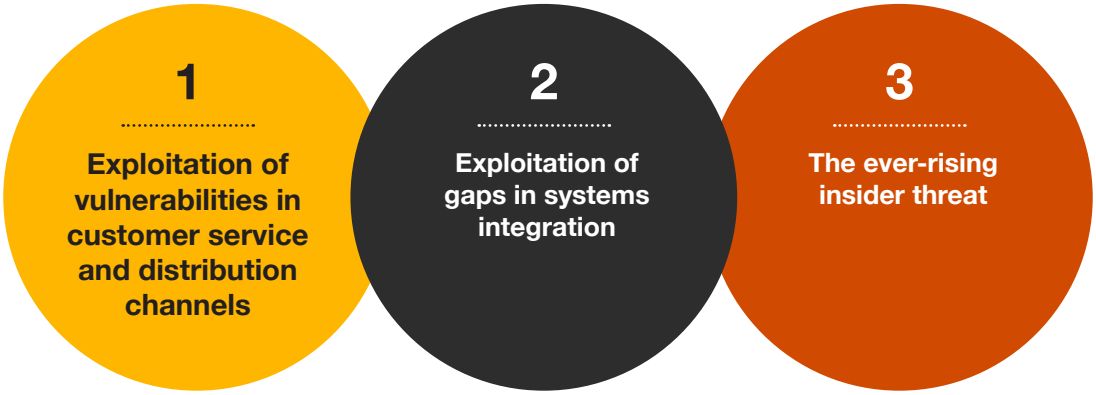
Globally, **cybercrime is now reported as the most experienced form of economic crime** at an incident rate of 44% and as the **most disruptive by 40% of the respondents.** In Uganda, the reported incident rate was 37%, two percentage points above the Eastern Africa average of 35%. 37% of the Uganda respondents also assessed cybercrime, alongside, customer fraud as the most disruptive economic crime in Uganda.

As evidence of the evolving and interconnected economic landscape, cybercrime incident rate that ranked a distant eight (8) in the GECS 2020 Uganda report with an incident rate of 12% has now **leap-frogged other forms of surveyed economic crimes to rank as the second most experienced form of economic crime in Uganda** at an incident rate of 37%, as is the global trend.



We recently published a digest on the cyber fraud landscape[3] where we covered our learnings from our recent cyber incidence response engagements in the financial services sector in Eastern Africa. Based on the reviews undertaken over the period, we mapped the below as the threat vectors driving cyber fraud incidents in the region:

The Cyber Fraud Threat Landscape



In an earlier digest[4], we also highlighted the rising cases of spoofing schemes as observed in the course of our work advising clients on managing and responding to various fraud and cyber-crime risks. The observed schemes primarily affected Non-Governmental Organisations (NGOs) and organisations with nascent finance functions. Spoofing is the disguising of communication by fraudulent actors to impersonate known/trusted sources. Common forms of spoofing involve fabrication of email addresses, websites and phone calls and with AI algorithms like generative adversarial networks (GANs), production of deceptive contents like “deepfakes” for impersonation.

[3]PwC EMA Forensics Digest: The Cyber Fraud Threat Landscape
[4]PwC EMA Forensics Digest: Noted increase in invoice fraud spoofing incidents in the Eastern Africa region

Our global cyber response teams have also analysed how new technologies and systems, including artificial intelligence (such as machine learning and generative AI), are being exploited for fraudulent activities and mapped the exploitation trends as below:

- **Reconnaissance and targeting** where AI tools are used to conduct reconnaissance on target organizations, their operations, and employees. This information is then used to inform attacks through exploitation of vulnerabilities, disinformation campaigns, and social engineering.
- **Exploitation of AI Tools** such as customer-facing chatbots and tools that are targeted with the aim of stealing sensitive information like proprietary data, biometrics, and user behaviour analytics.
- **Adversarial Machine Learning** through techniques like "poisoning" training data, jailbreak prompts and prompt injection attacks to degrade the detection and defensive capabilities of AI-based cybersecurity systems.
- **Use of deepfakes and synthetic media** for phishing/ vishing campaigns, business email compromise (BEC), extortion, disinformation, and generation of harmful content.
- **Malware Development** using AI tools like FraudGPT and WormGPT. Polymorphic malware can change its code to avoid detection, making it harder for traditional antivirus solutions to identify.
- **Espionage** where state-sponsored actors use AI tools for intelligence collection and AI technologies themselves targeted to steal sensitive information about users and the broader tech ecosystem.

Insights from other relevant publications/ statistics

PwC's Eastern Africa 2024 CEO Survey cites cybercrime as an increasing area of concern with 28% of CEOs citing it as a threat up from 22% in 2023.

The Uganda National Information Technology Authority (NITA-U)'s 2022 national information technology survey report highlighted that the expanding digital landscape had made both individuals and organisations vulnerable to cyberthreats.

The report findings include a noticeable lack of awareness and understanding of cybersecurity risks among many users, contributing to higher susceptibility to cyber threat.

Where to from here?

Anticipate and prepare, don't just react!

It is critical that organisations adopt a holistic approach to cyber fraud security that combines technology, training, and proactive incident response strategies to protect their digital assets and sensitive information. Cybercrime incidents should also be adequately investigated.

[5]PwC's Eastern Africa 2024 CEO Survey report

[6]Uganda National Information Technology Authority (NITA-U)'s 2022 national IT survey report

Procurement Fraud

As assessed by 23% of the respondents, procurement fraud completes Uganda's top three (3) most disruptive economic crimes behind customer fraud and cybercrime discussed above.

At an incident rate **26%**, procurement fraud is the **fourth most experienced form of economic crime in Uganda** behind customer fraud, cybercrime and asset misappropriation in that order.

89% of respondents reported procurement fraud as widespread in the country.

Globally, the **highest** incident rates of procurement fraud are reported in the **Energy and Resources Sectors and Government and Public Sector** with the Financial Services sector reporting the lowest incident rate at 8%.

Uganda's incident rate of procurement fraud could therefore be understated as the Uganda's respondents were biased towards the financial services industry at a response rate of 63%.

32%	30%	29%	27%	23%	20%	8%
Energy, Utilities & Resources	Government & Public Sector	Industrial & Manufacturing	Health services	Consumer Market	Technology & Media	Financial Services

Procurement fraud has been the traditional avenue for extraction of financial value from organisations due to its historical prevalence and opportunity for substantial rewards for fraud.

High financial stakes:

High value financial transactions and opportunities for budget manipulation

Complexity and Opacity:

Complex, multiple steps, often involving multiple stakeholders

Opportunities for collusion:

Bid rigging, bribery, invoice kickbacks and conflicts of interest

Insights from other relevant publications/ statistics

As noted above, there exists a strong interplay between procurement fraud and corruption. The highlighted opportunities for collusion including bid rigging, bribery, invoice kickbacks and conflicts of interest are corruption schemes.

At an incident rate of 26% in Uganda and 24% globally in our current survey, **bribery and corruption continues to be a big challenge globally** and a driver of some of the other schemes. **52%** of the respondents in Uganda indicated that the **risk of corruption has been increasing and 63% reported that government efforts to enforce anti-corruption laws were either not changing/ improving or were becoming less aggressive.**

Where to from here?

Make fraud risk more visible across the organisation

Managing procurement fraud risk requires involvement of staff across the enterprise, not just procurement; and includes user departments, compliance, investigations, and audit functions. This calls for initiatives such as training and increased awareness, reliable whistle-blower channels, risk assessments, market surveys, data analytics and automation, robust vendor due-diligence and conflict of interest checks.

Other risk areas of interest

From review of the statistics, Uganda respondents either reported limited awareness or appeared to be reporting more incidents as compared to regional and global rates in these specific categories.

Environmental, Social, and Governance (ESG)	Insider/ unauthorised Trading
73% of Uganda respondents had either not heard of or studied the Corporate Sustainability Reporting Directive (CSRD) and its potential impacts to their businesses. CSRD is part of the European Union's broader strategy to improve sustainability reporting and promote ESG practices. It includes reporting on human rights practices and the steps taken to prevent forced labour within their supply chains.	At 17%, the reported insider trading incident rate is higher than the Eastern Africa average of 11% and 2X the global average of 8%. This trend was also observed in the 2020 survey.

Environmental, Social, and Governance (ESG)

The Corporate Sustainability Reporting Directive (CSRD) was formally adopted by the European Parliament on 10 November 2022 and all EU member states are required to have transposed it into national law by end of July 2024. This year will therefore be the first reporting year under the CSRD framework, and its provisions will begin to be felt going forward.

Why is this relevant to Uganda?

To comply with CSRD requirements, companies will need to demonstrate that they have effective due diligence processes in place to identify, assess, and address issues such as forced labour in their supply chains. These guidelines should be read together with the EU's Forced Labour Regulation (FRR) adopted in April 2024 and expected to also come into force within the year after publication in the EU official journal.

The forced labour regulations complement the CSRD by enforcing stricter controls and due diligence requirements on companies to ensure their supply chains are free from forced labour. The regulations specifically target products made with forced labour and aims to ban them from being imported into or exported from the EU market. 88% of the respondents in Uganda had either never heard of or never considered assessing compliance with forced labour regulations.

With the EU taking up 21% of Uganda exports valued at EUR 800M as of May 2024, Uganda based organisations, especially those in the export sectors, should therefore take note of the developments and assess the potential impact to their organisations.

Globally and from the survey results, organisations are taking note of the shift and 55% of the respondents reported that their organisations are prioritising assessing the risk of forced labour in their supply chains. 26% of the respondents indicated that their organisations would adopt third-party audits regarding forced labour "because it is the right thing to do" signifying a substantial buy-in already.

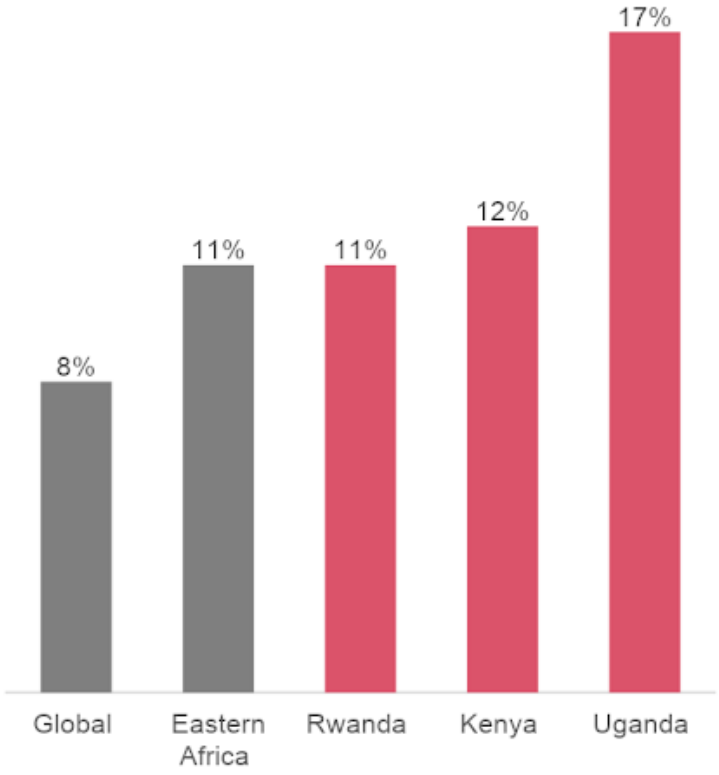
It is also likely that similar forced labour regulations will be adopted by other countries, much like how the EU General Data Protection Regulation ("GDPR") influenced global data privacy laws. Several countries, including Australia, Canada, Germany, the United Kingdom and the United States, have already implemented or are developing their own forced labour regulations.

Insider/ unauthorised Trading

Though the statistic may be driven by the bias of financial services respondents in Uganda, we find this to be a significant incident rate worth looking into.

Looked at against two of its close neighbours, Kenya and Rwanda that appear to be oscillating around the Eastern African average of 11%, **Uganda appears to be pulling away in the number of recorded incident rates at five percentage points above the regional average and 2X the global average.**

Consideration should be made on the potential driver of the high incident rate in Uganda including drawing lessons from comparable markets where applicable. This can be done as part of the reflections on the implementation of Uganda Capital Markets Master Plan (2014–2023) and requisite measures considered in the next blueprint.



How are organisations in Uganda fighting fraud

We asked our respondents on what they are doing to mitigate fraud risks. We highlight below the good practices noted and the areas that might need improvement.

The good

64%
16% planned to undertake one in the coming 12 months

Organisations had conducted an enterprise-wide fraud assessment in the last 12 months. This is higher than the reported number globally at 59% and the Eastern Africa average of 53%. **14%** of respondents had not conducted enterprise-wide fraud risk assessment in the last 12 months.

61%
27% leverage data aggregation technologies to assess effectiveness of their compliance programs

Organisations undertake root cause analysis and apply lessons learned to improve their organisation's compliance programmes following instances of fraud, bribery or other improper conduct. This was higher than the global rate of 44% and 52% from Eastern Africa. Only 9% reported not undertaking this analysis.

50%
29% do ad hoc retrospective analysis of transactions

Organisations undertake continuous monitoring of certain transaction types to support their compliance functions. This was higher than the global rate of 41% and 44% from Eastern Africa. **20%** of respondents do not use data analytics to support the compliance function.

What we need to do better

83%
5% were either unsure or did not know

Indicated that anti-bribery / anti-corruption audits are rare or none had been undertaken in the last two years. 13% reported as regularly conducting anti-bribery / anti-corruption audits of third parties.

70%
20% have a third-party risk management programme but corruption risk is not a factor

Organisations either do not have a third-party risk management programme or do not do any form of risk scoring as part of their programme. 30% reported having a third-party risk management programme which incorporated corruption risk as a factor in the scoring process.

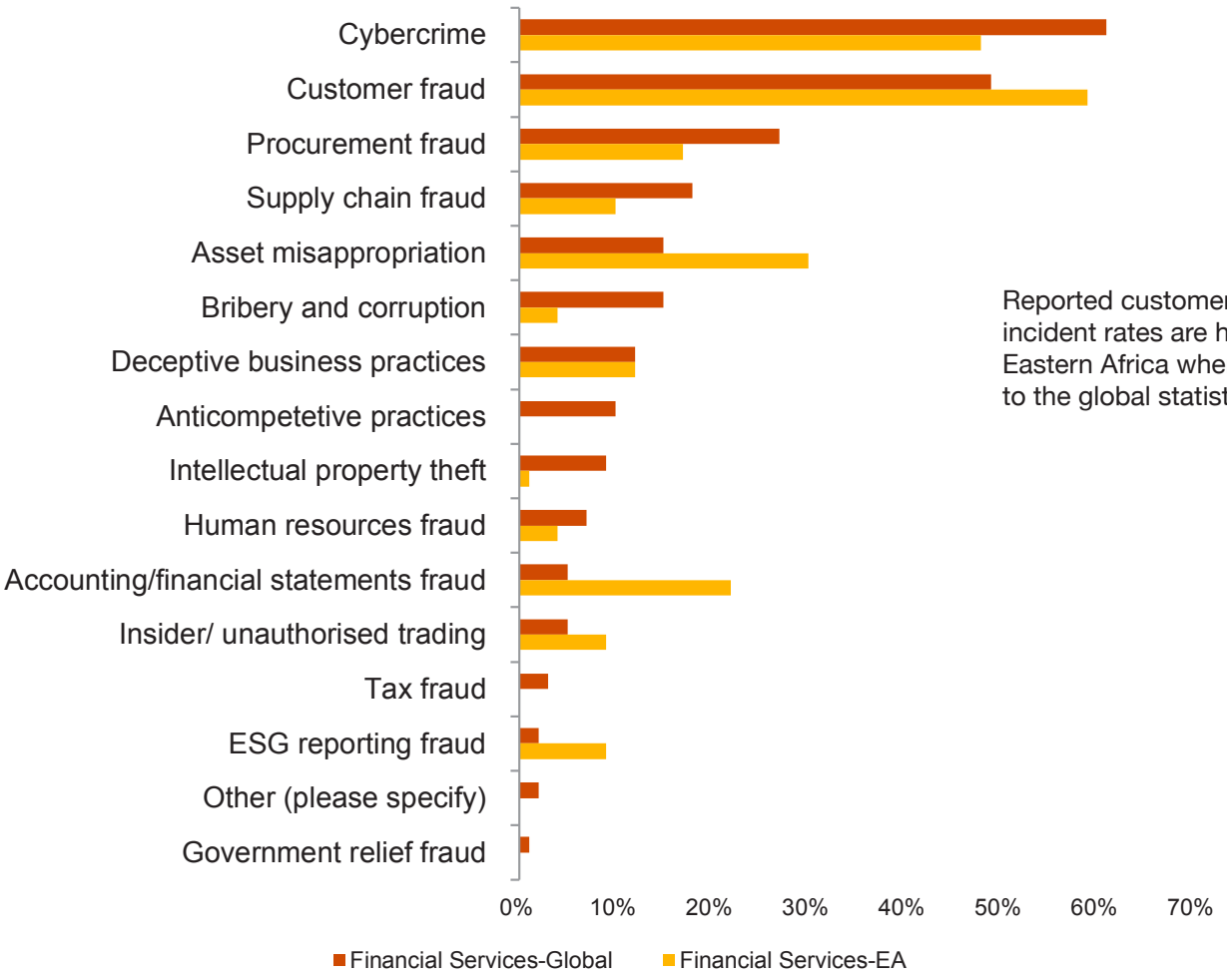
63%
7% were either unsure or did not know

Respondents view government efforts to enforce anti-corruption laws as either not improving or are becoming less aggressive. This is as compared to 49% and 52% in Eastern Africa and Globally respectively. 30% reported that government efforts are becoming more robust.

Industry Insights – Schemes with the highest incident rates by industry/ sector

We highlight the most prevalent forms of economic crime by industry/ sector based on the analysis of the global results and provide examples of some of the schemes observed in the Eastern region in the course of our work.

Financial services - Consistent with the Uganda and Eastern Africa results, the most prevalent schemes in the financial services sector are customer fraud and cybercrime.



Reported customer fraud incident rates are higher in Eastern Africa when compared to the global statistics.

Cybercrime fraud schemes:

1. Phishing
2. Identity theft
3. Insider threats
4. Ransomware attacks
5. Spoofing

Customer fraud schemes:

1. Account takeover of mobile money and traditional bank accounts
2. Fake customer profiles
3. Identity theft
4. Credit fraud in trade finance instruments

Industry Insights – Schemes with the highest incident rates by industry/ sector

Government & Public Sector - Globally, bribery and corruption is reported as the most prevalent form of economic crime in the government and public sector. This is consistent with observations from our work in Uganda and the Eastern African region

Asset Misappropriation

1	Inventory pilferage
2	Cash larceny
3	Expense reimbursements
4	Misuse of organisational assets like vehicles

Bribery and Corruption

1	Favoritism in recruitment and staff contract renewals
2	Procurement fraud
3	Bid rigging
4	Extortion, facilitation fees and kickbacks
5	Illegal gratuities, honoraria or allowances
6	Diversion of funds/ assets for personal use
7	Trading in influence

Industry Insights – Schemes with the highest incident rates by industry/ sector

EUR & IM - Potentially driven by the high capital expenditure vote, procurement fraud is reported as having the highest incident rate in the Energy, Utilities and Resources sector followed by cybercrime. This is replicated in the Industrial and Manufacturing sector where cybercrime closely edges out procurement fraud.

Energies, Utilities and Resources

Industrial and Manufacturing

Procurement fraud schemes:

- Bribery and kickbacks
- Bid rigging and bid splitting
- Conflict of interests
- Invoice fraud include fictitious orders and over-invoicing
- Change order abuse
- Accounting fraud

Cybercrime schemes:

- Supply chain attacks
- Insider threats
- Phishing
- Ransomware attacks

Industry Insights – Schemes with the highest incident rates by industry/ sector

Consumer Markets/ TMT - Similar to financial services, use of digital channels appears to be driving cybercrime and customer fraud incidents in the consumer markets (retail, FMCG, hospitality and leisure, and transport and logistics) and the Technology, Media and Telecom sectors.

Consumer Markets

Technology, Media and Telecommunication

Customer fraud schemes

1. **1** - Inventory pilferage
2. **2** - Use of post-dated cheques
3. **3** - Credit fraud in trade finance instruments
4. **4** - Misuse of trade rebates
5. **5** - Misuse of refund processes and sales promotions to extend undue credits to conflicted customers

Cybercrime fraud schemes

1. **1** - Phishing/ Vishing and social engineering
2. **2** - Business email compromise
3. **3** - Identity theft and imposter scams
4. **4** - Ransomware attacks
5. **5** - Consumer fraud including non-delivery scams
6. **6** - Supply chain attacks

Conclusion and recommendations

We highlight below the key takeaways from the survey results:

a. Technology appears to have facilitated a paradigm shift in the nature of economic crimes with digital channels now being at the forefront as both tools and avenues to perpetrate economic crimes evidenced by the rise in cybercrime and customer fraud incident rates. This includes use of new technologies and systems, including artificial intelligence such as machine learning and generative AI.

b. Procurement fraud, bribery and corruption risks remain persistent challenges. 89% of respondents perceive procurement fraud as widespread in the country while 52% indicated that the risk of corruption has been increasing. 63% reported that government efforts to enforce anti-corruption laws were either not changing/ improving or were becoming less aggressive.

c. As business evolve to meet the demands of modern consumers, so does the regulatory environment. We are now seeing an increased emphasis on ESG with a specific lens focused on issues such as forced labour in supply chains. As such, Uganda based organisations also need to evolve and assess potential exposure as compliance measures are enforced globally.

It is encouraging that Uganda is ahead of the curve in deploying enterprise-wide fraud risk assessments and related fraud risk management measures, results of which will be visible increased awareness, detection, and deterrence. The good practices need to be reemphasized and reinforced.

Internally, organisations should continuously update their risk registers including now developing and assessing fraud typologies associated with the changes in their operational and control environments such as heightened corruption risks and the changes brought about by the current technological transformation like AI.

Fraudsters are also mobile and have the ability to replicate schemes from one organisation to the other either individually or through a network of collaborators. How well do industry players share information on appropriate trends, known risks and anti-fraud strategies? As an example, the Uganda Bankers Association has taken a lead with the annual fraud forum which brings together key stakeholders in the public and private sector to have candid discussions regarding the threat faced by the banking industry. It would be appropriate to take stock of its successes and challenges and consider how the learnings can be applied to other sectors such as fraud in the insurance sector and corruption in both the private and public sectors.

Uganda Forensics leadership team

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 team of dedicated specialists has conducted some of the most complex and high-profile investigations undertaken in Uganda and regionally in recent years.

Contact us

Uthman Mayanja
Country Senior Partner,
PwC Uganda
uthman.mayanja@pwc.com

Patrick Matu,
Associate Director,
Forensics Services,
PwC East Market Area
patrick.k.matu@pwc.com

Johnstone Mwendwa
Senior Manager,
Forensics Services,
PwC East Market Area
Johnstone.mwendwa@pwc.com

Doreen Mugisha,
Manager,
Clients and Markets Development,
PwC Uganda
doreen.mugisha@pwc.com

EMA Forensics management team

Muniu Thoithi,
Partner, Forensics Services,
PwC East Market Area.
muniu.thoithi@pwc.com

John Kamau,
Partner,
Forensics and Lead Financial Crime,
PwC East Market Area.
john.kamau@pwc.com

George Weru,
Partner, Forensics Services,
PwC East Market Area
george.weru@pwc.com

Chrisantus Khulabe,
Senior Manager, Forensics Services,
PwC East Market Area.
chrisantus.khulabe@pwc.com

Johnstone Mwendwa,
Senior Manager, Forensics Services,
PwC East Market Area
Johnstone.mwendwa@pwc.com

Brenda Guchu,
Senior Manager, Forensics Services,
PwC East Market Area
brenda.guchu@pwc.com

Hazel Woodhead,
Manager, Forensics Services,
PwC East Market Area
hazel.w.woodhead@pwc.com

Pamella Williams,
Manager, Forensics Services,
PwC East Market Area
pamella.w.williams@pwc.com