KPMG

Banking Fraud Risks

The multi-faceted threat of fraud: Are banks up to the challenge?

July 2019

Survey: Purpose & Scope

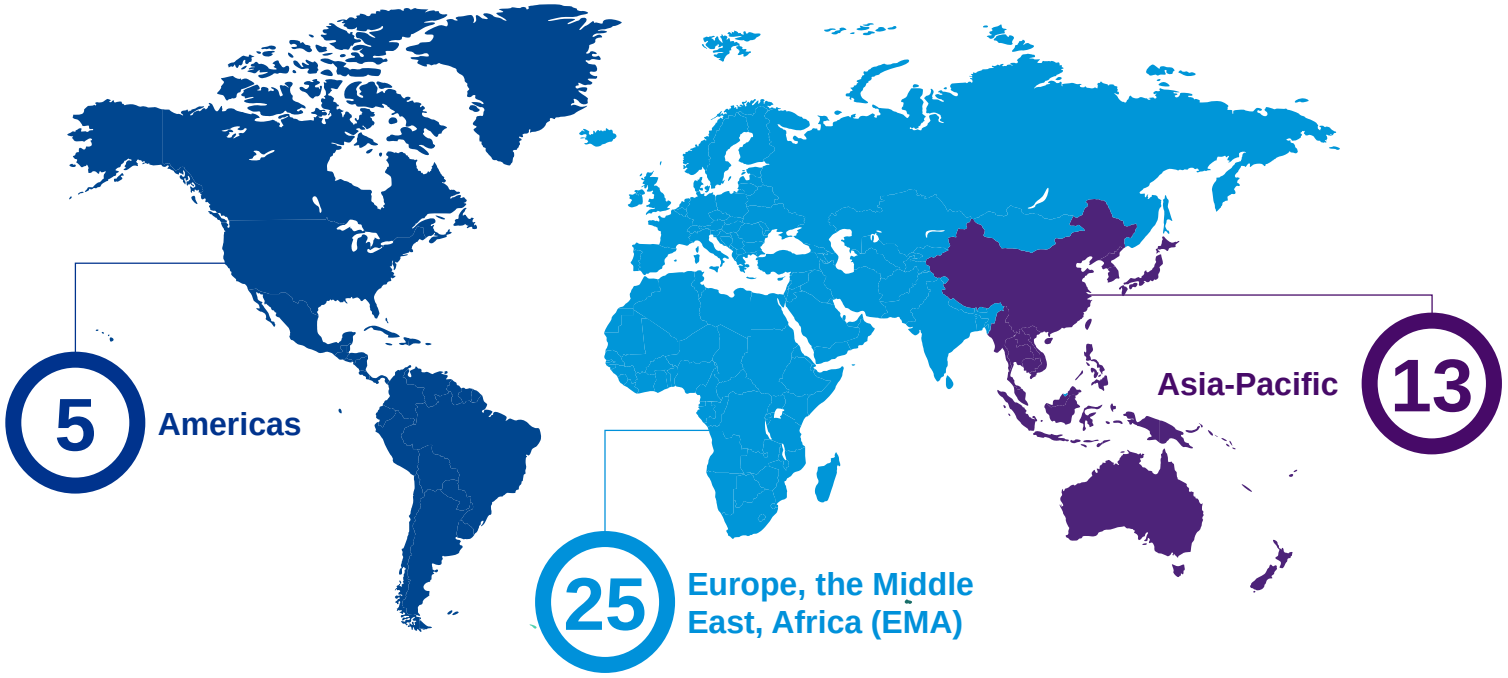
Purpose:

To gain insight into global trends and regional differences in how banks are identifying, assessing and addressing fraud risk.

Scope:

KPMG's Global Banking survey was conducted between November 2018 and February 2019 across 43 retail banks.

18 have annual revenues in excess of US$10 billion & 31 each employ more than 10,000 people across the globe.



Key Findings

Typologies

Card not present (“CNP”)

Identity theft

Scams

Cyber/ online fraud

Security in a Digital World

Increasing products delivered via digital channels

Rules, machine learning techniques/AI and robotics

High volume of false positives

Investment vs Costs

Complex operating models

Non-agile processes

Customer education

Here and now’ as opposed to predicting emerging trends

Fraud Operating Model

Lack of a documented Fraud Operating Model and enterprise wide Fraud Risk Assessment

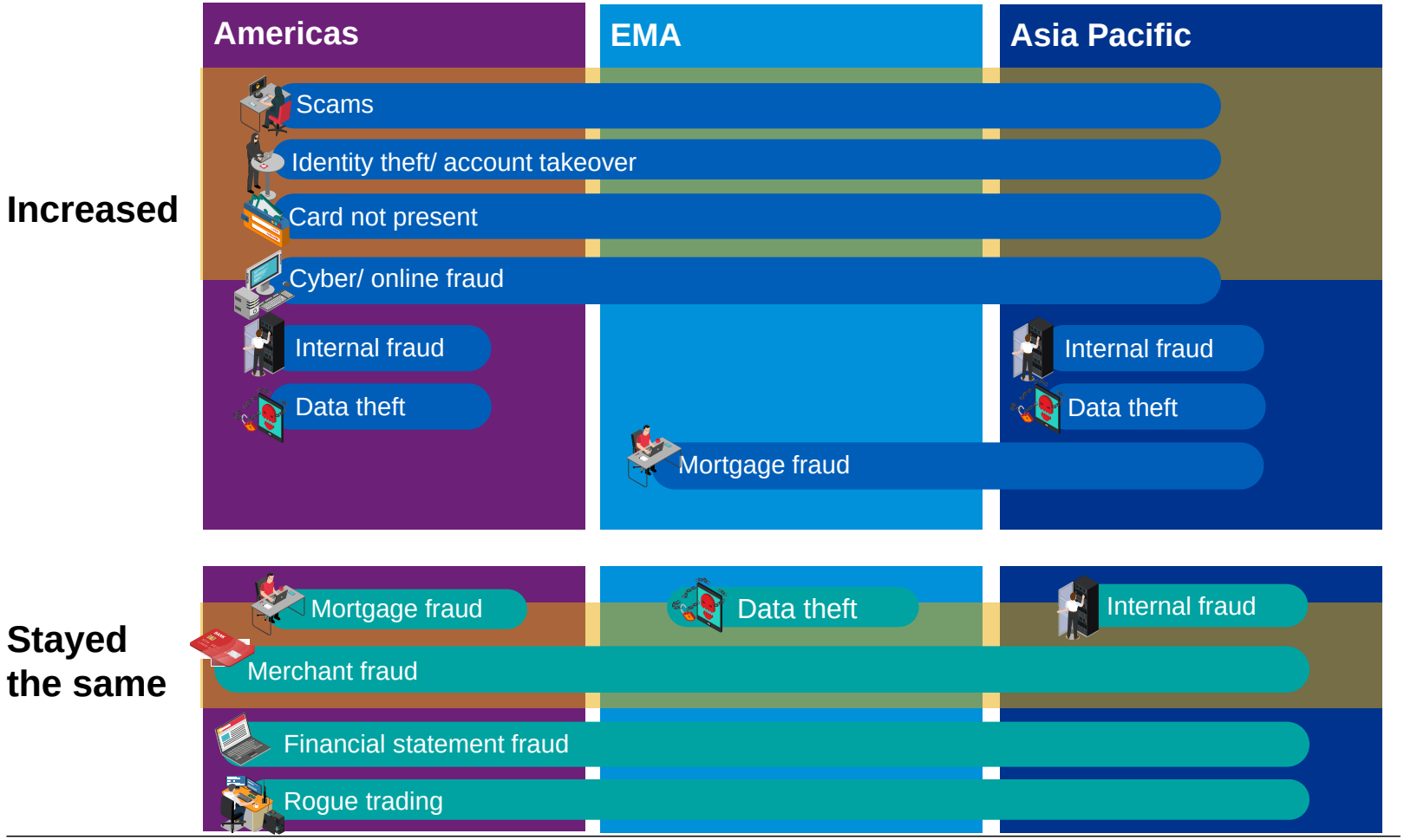
Failures to detect impact management information and investment decisions

Optimizing technology versus headcount

Financial crime operations in silos

Regional fraud trends by typology

Survey fraud typology trends by region 2017-2018 based on the most common response



Challenges facing banks globally in mitigating fraud risk

AMERICAS

1. Cyber and data breaches
2. Faster payments
3. Open Banking (equal third)
4. Evolving digital channels (equal third)
5. Virtual currencies (equal third)

EMA

1. Cyber and data breaches
2. Faster payments
3. Evolving digital channels
4. Payments Services Directive 2 (PSD2) / Open banking
5. Social engineering

ASIA PACIFIC

1. Cyber and data breaches
2. Social engineering
3. Faster payments
4. Evolving digital channels
5. Open Banking

Source: Global Banking Fraud Survey, KPMG International 2019

We look at these challenges in more detail below

1. Cyber and data breaches

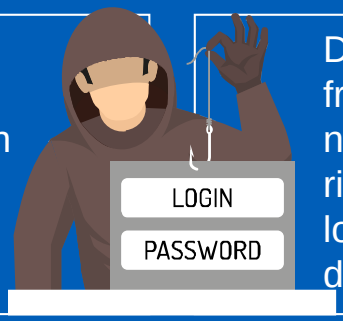
2. Social Engineering

3. Evolving digital channel & Faster payments

4. Open Banking

1 Cyber & data breaches

Cyber criminals are obtaining access to personal data, via data breaches, and using personal information to gain a customer's trust in scams or takeover their account.



Digital transformation is changing fraud typologies. To respond banks need to be agile to update their fraud risk frameworks, hone technology & look to next gen prevention & detection solutions.

Customer data/records now in public domain

Target **110 million** people in 2013

Yahoo **3 billion** & **500 million** accounts in 2013 and 2014 respectively

Ebay **145 million** user in 2014

Adult Friend Finder Networks **412 million** accounts in 2016

Equifax **148 million** people in September 2017

Chinese Huanzhu Hotels Group **500 million** records in August 2018

Facebook **50 million** accounts in September 2018

Marriot International **500 million** records in December 2018

Source: Global Banking Fraud Survey, KPMG International 2019

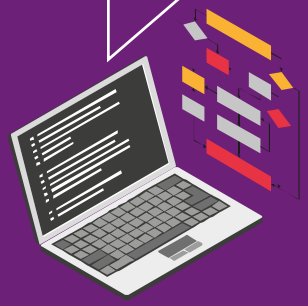
Staying a step ahead of fraudsters....

Fraudsters are catching on to:

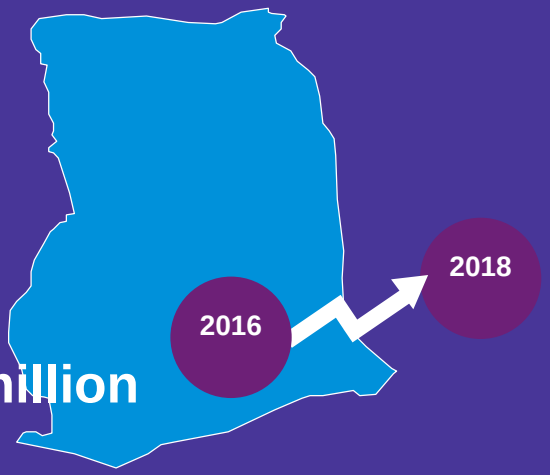
1. Data security
2. Step up SMS authentication with phone porting
3. IP masking
4. Phone spoofing of legitimate business
5. Voice recognition via technology developed to replicate voice and scammers have attempted to record victim's voices to bypass voice recognition
6. Finger print biometrics and customer personal data, sourcing these from cyber market places
7. Phishing, scams to increase their success rate/ returns via attacks at scale

What is next gen fraud detection?

- Combined technologies to form a robust prevention & detection, supported by a robust fraud operating model
- Real time rules and machine learning
- Behavioural biometrics, including to the extent this can be used for scam detection
- Educating customers



2 Social engineering: a spotlight on scams

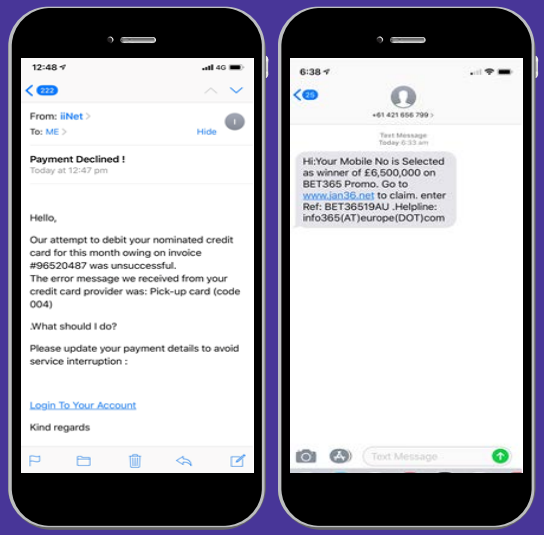


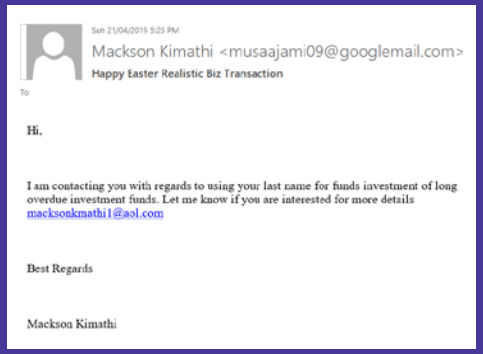
$97 million

Ghana lost US$97m to cybercrime related activities between 2016 – 2018, with only 5.7% of the reported fraud cases undergoing investigations, Director of the Cyber Crime Unit of the Criminal Investigation Department (CID), Dr. Herbert Gustav Yankson, has revealed

Source: BF&T October 2018

- 2018 almost half a billion in scam losses
- New tricks are being employed by fraudsters
- Scam victims vary
- Banks are often blamed, dedicating significant resources to manage customer scam situations & finding conflict when customers are convinced of a scams legitimacy.
- In Ghana, there is no clear liability framework, and different approaches are being taken by banks – to compensate or not to compensate, that is the question.





2 Social engineering: a spotlight on scams (cont.)

Authorized Push Payments (APP) Fraud

Value £354.3m

50%

Volume 84,624

93%

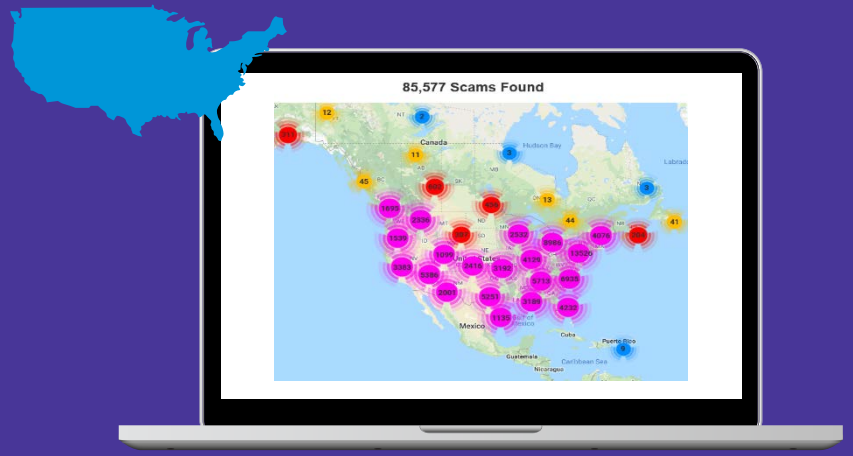
A total of £1.66 billion of unauthorised fraud was prevented by the banking and finance industry in 2018.

However, a total of £1.2 billion was stolen by criminals committing fraud last year, comprised of:

— £354 million in authorised fraud (scams)

— £845 million in unauthorised fraud

Source: UK Finance report 'Banking industry prevented GBP1.66 billion of fraud in 2018



Source: BBB scams tracker reporting North America & Canadian scam incidents reported by victims & potential victims between 1 May 2017 to 1 May 2019

Contingent reimbursement model code for APP scams

— Code in Force from 28 May 2019

— Agreed principles for greater protection of customers and the circumstances in which they will be reimbursed.

— Reimbursement will occur if the customer was a victim of an APP scam, followed standards expected by customer but provider did not.

Source: BBB scams tracker , 2015 to December 2018

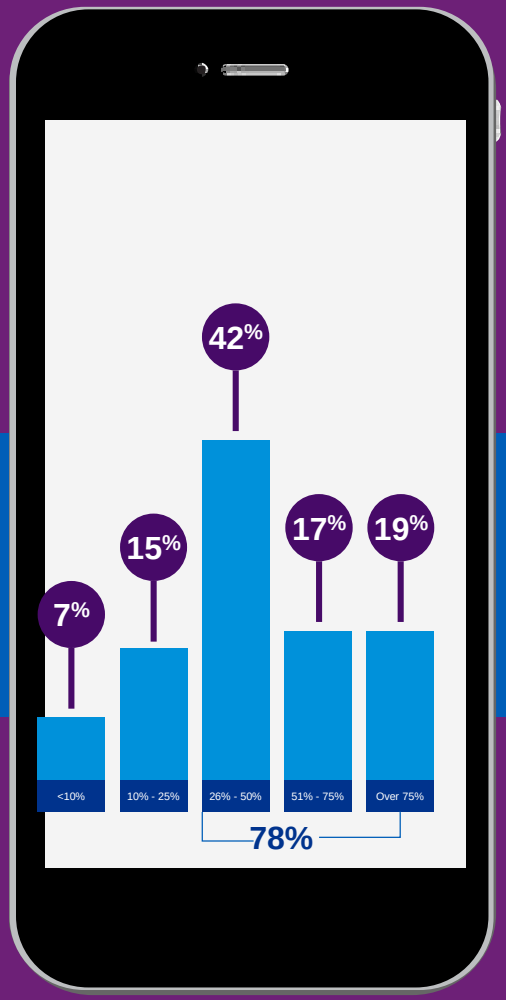
3 Evolving digital channels & faster payments

— The survey found 78% of respondents reported over 25% of their products & services are delivered via digital channels.

26th Society for Worldwide Interbank Financial Telecommunication (SWIFT) Africa Regional Conference – June 2019, Accra

Ghana Will Tackle Cyber Attacks, Digital Fraud - President Assures – Ghanaian Times, 19 June

" He said for instance, mobile money penetration in Ghana was the second in Africa, with mobile money transactions amounting to GH¢213 billion in 2018, up from GH¢78.8 billion in 2016."



— Reducing the face to face interaction between banks and their customers, which is being exploited by organized criminals and fraudsters to commit fraud across borders.

+ Providing a rich data set of customer digital behavior, making it easier to spot potentially fraudulent payments.

— Dr. Ernest Addison, the Governor of the Bank of Ghana, on Tuesday said the Payment Systems and Services Act 2019 will help to create an enabling environment for the on-going digitisation processes in the economy. He said the implementation of the Act would help liberalise the country's payment system further and allow for the entry of non-banks, direct licensing of FinTechs by the Bank of Ghana and ultimately promote financial inclusion to facilitate electronic means of payment.

— With a move to pull payments, vigilance to increased fraud is required. Particularly as lower recovery rates are expected given the velocity of faster payments.

4 Open Banking

Open Banking is likely to impact fraud risk with:

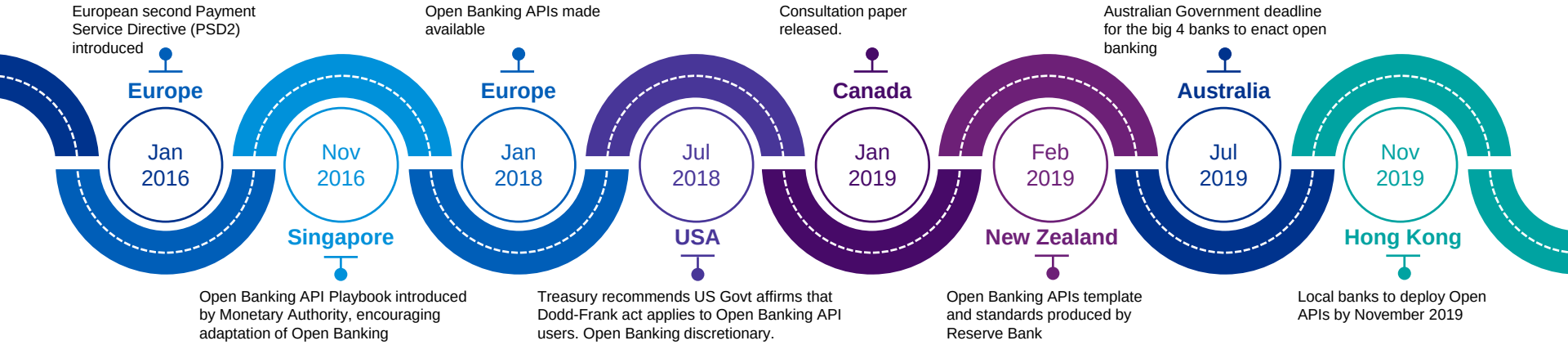
likely higher transaction volumes for fraud detection;

reliance on the security of third parties to protect customer banking information accessed through Application Programming Interfaces (APIs); and

fraudsters who gain access, to gather more sensitive customer data, presenting a more holistic picture of a customer's accounts to target liquid accounts across banks.

On the flip side, for banks this greater transparency of their customers' accounts across banks will likely enable more robust identity verification, the earlier identification of mule/ fraudulent accounts and more efficient fraudulent funds tracing given the visibility of a customer's accounts across banks.

A summary Open Banking timeline across the globe



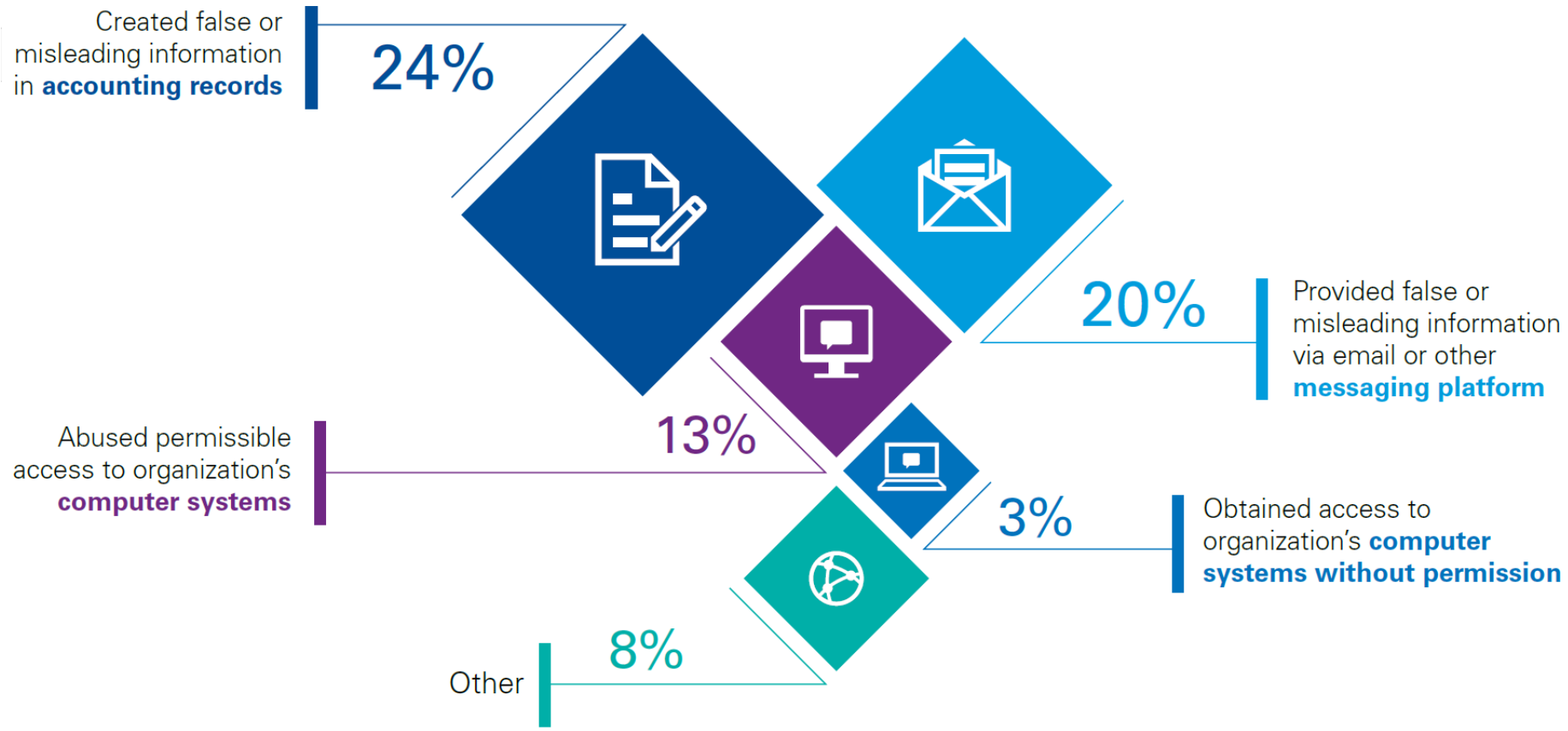
Preparing for Open Banking from a fraud risk perspective

Data security Digital identity Access management

KPMG

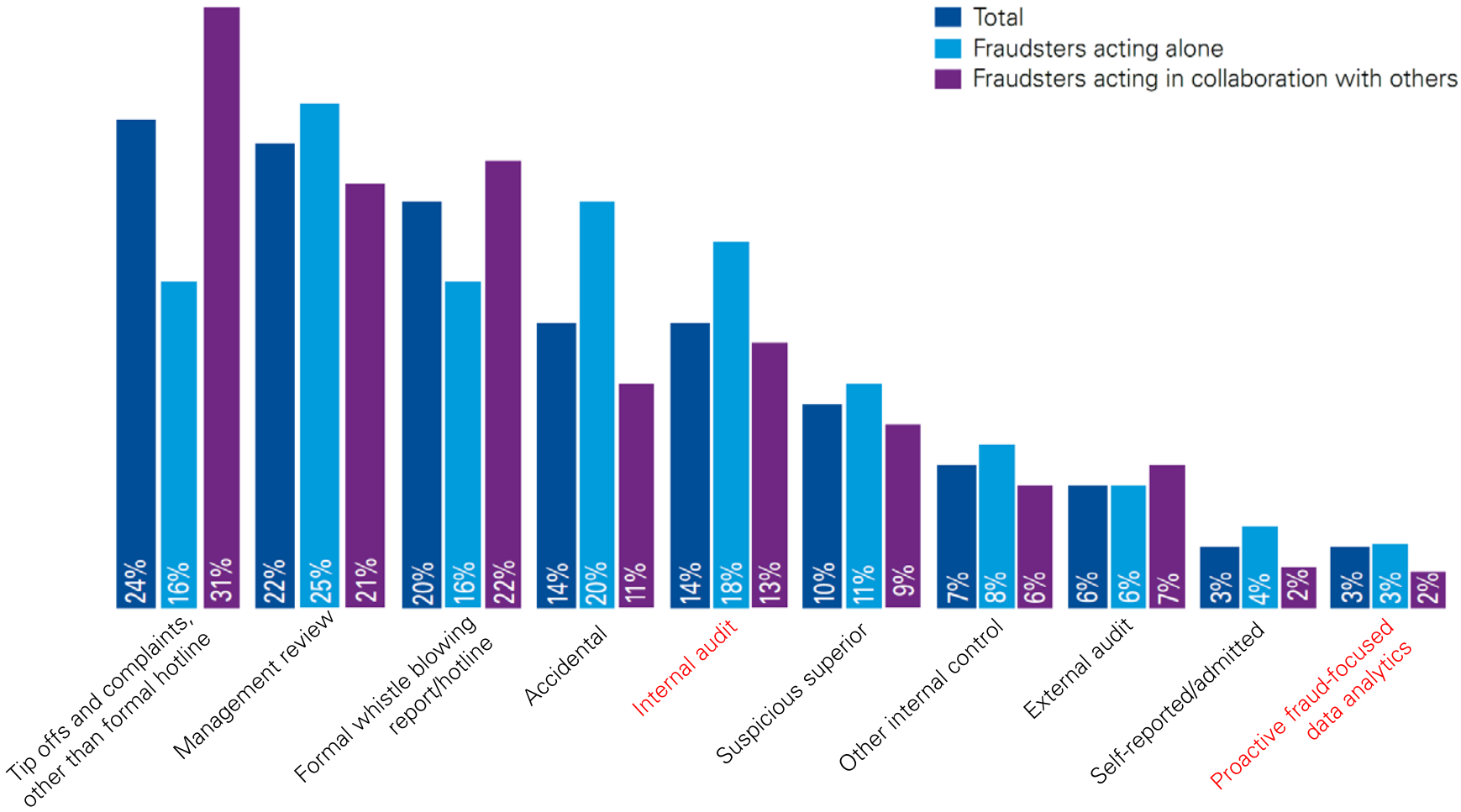
Fraud Detection

How technology was used to perpetrate the fraud



Source: *Global Profiles of the Fraudster*, KPMG International 2016

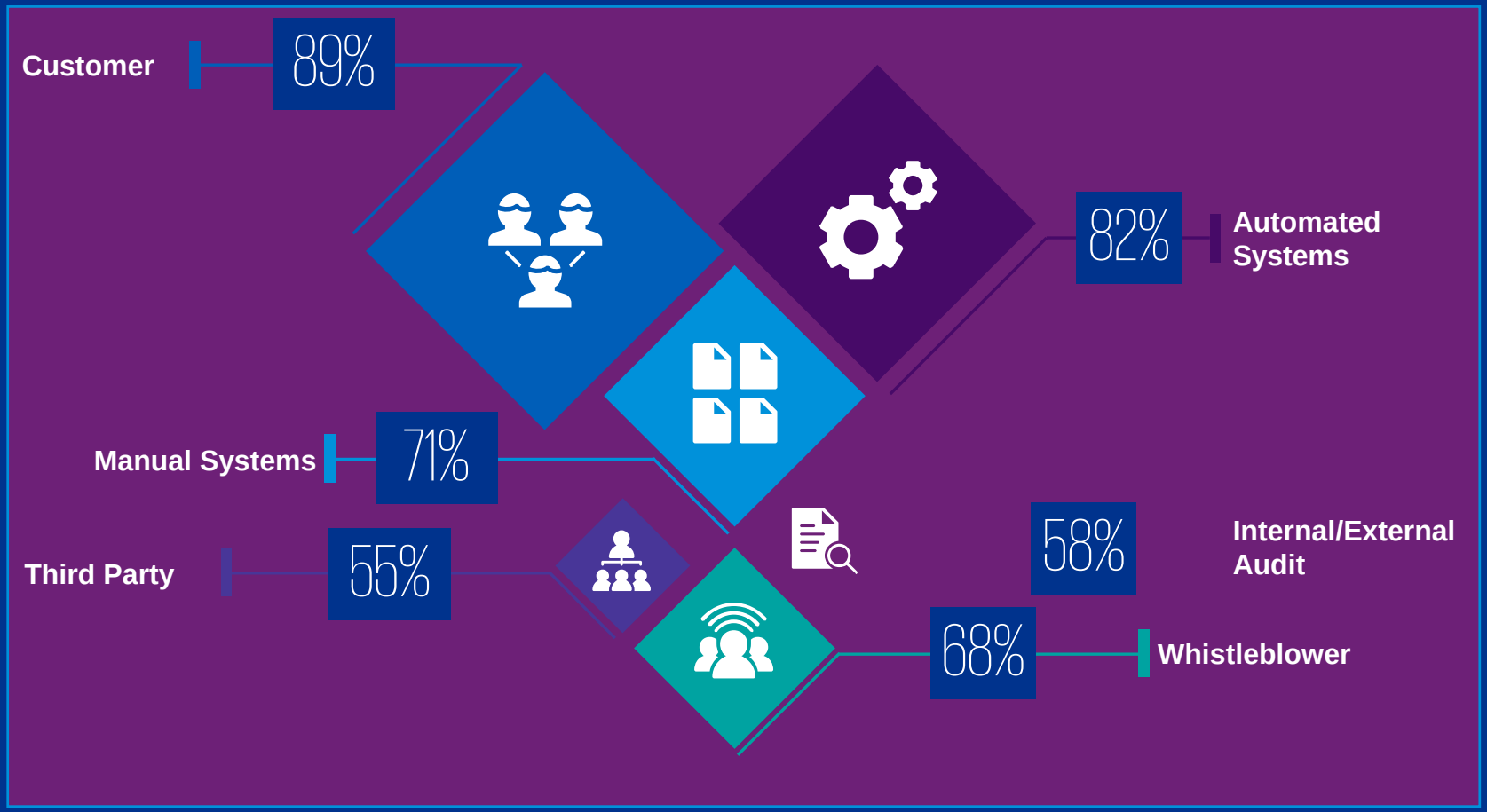
How the frauds were detected



Source: *Global Profiles of the Fraudster*, KPMG International 2016

Fraud detection & customer education

How do banks identify fraudulent activity?



Source: Global Banking Fraud Survey, KPMG International 2019

The fraud operating model- survey findings

Documentation

Around a third of banks surveyed do not have a documented Fraud Operating Model, conduct enterprise wide risk assessments and / or a good understanding of how much fraud risk management efforts cost the bank

Integration

42% of banks do not have any software, staff, reporting or governance integrated between fraud and financial crime

False positives

A diversity in fraud systems was reported, with most using proprietary builds. 51% reported significant false positives from their fraud prevention & detection technology

Cost v benefit

More than half of banks surveyed don't record the total cost of fraud risk management for their Bank annually.

No common fraud operating model

Fraud reporting lines and accountability responses were diverse. 68% reported fraud risk as owned by the first line, and 32% by the second line.

KPMG's fraud navigator

KPMG has a developed a fraud navigator tool to assess the maturity of bank operating models holistically across governance, people, processes & technology.

Conclusion

Fraudsters are becoming more sophisticated and agile in their approach to diversify their efforts from CNP & social engineering/ account takeovers to scams where customers are the weak link.

The insider threat can be as great, if not greater than external fraud as they are privy to your systems and customer data.

Technology alone is not enough. There is a necessity to plan outside of technology to obtain efficiency and optimum performance (minimising false positives) across governance, people, processes in support of bank technology.

Banks must enhance their ability to analyse data within an open banking environment and navigate through API's.

77% of respondents plan to invest in the following technologies over the next three years:

- Transaction monitoring technology with machine learning / AI / robotics.
- Fintech / RegTech development.
- Biometrics and greater use of open source and social media data.

ANDREW AKOTO
Partner, Risk Consulting
KPMG in Ghana

T: +233 208174629
E: aakoto@kpmg.com

Designed by CREATE | CRT1129944