







Global Banking Fraud Survey

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

May 2019

kpmg.com

Content

	Foreword	04
	Key findings	05
	Themes of the survey	06
	The fraud operating model	15
	Conclusion	19

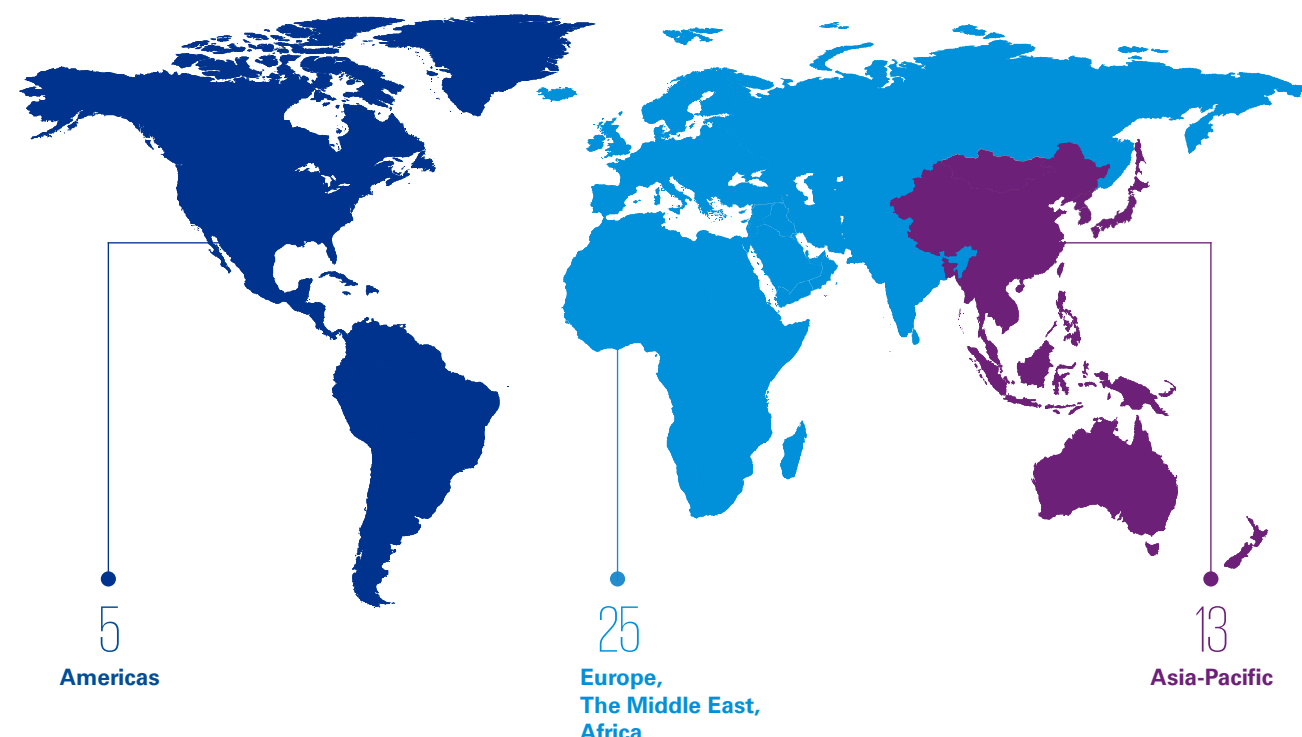
Foreword

KPMG is delighted to share the findings of our inaugural Global Banking Fraud Survey (Survey). The Survey was conducted to obtain a global perspective of how banks are tackling internal and external fraud threats.

The Survey questioned banking fraud risk, investigations and group security professionals on trends in fraud typologies, challenges banks are facing in mitigating internal and external threats in the period 2016 to 2018, security in a digital age and how banks are structuring their teams and deploying resources to optimize their fraud risk management efforts.

KPMG's Global Banking Survey was conducted between November 2018 and February 2019 across 43 retail banks, 13 of which are in the Asia-Pacific, 5 in the Americas and 25 in Europe, the Middle East and Africa (EMA) region. Eighteen have annual revenues in excess of US\$10 billion and 31 employ more than 10,000 people across the globe.

We would like to thank the respondents who took the time to participate in the survey. We are delighted to share the results, accompanied by our own global and regional insights from KPMG member firm professionals.



Source: Global Banking Fraud Survey, KPMG International 2019

“Our survey has identified that fraud costs are increasing at a faster rate than fraud risk management spend. A radical rethink is urgently required.”



David Hicks
Global Forensic Leader
KPMG International

Throughout this document, “we,” “KPMG,” “us” and “our” refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

© 2019 KPMG International Cooperative (“KPMG International”). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated.

Key findings

- Over half of survey respondents globally experienced increases in both external fraud total value and volume. Increasing fraud typologies globally from 2015 to 2018 include identity theft & account takeover, cyber attack, card not present fraud and authorized push payments scams. In this report we refer to such customer authorized payments as scams.
- The largest portion of respondents globally said that the total cost, average cost and volume of internal employee fraud detected stayed the same or decreased. This may not, however, present a true picture of the cost of internal fraud. Many external frauds originate with someone working inside the bank.
- Over half of respondents recover less than 25 percent of fraud losses; demonstrating that fraud prevention is key. Banks are investing in new technologies, including machine learning real time fraud alerts, voice, facial & fingerprint recognition (biometrics) and profiling how customers interact with their device and internet banking (behavioral biometrics) towards fraud prevention.
- In every region, banks surveyed considered the most significant challenge in fraud risk to be cyber attacks. Fraudsters are obtaining customer data through hacking, in social engineering attempts, on the dark web and through criminal networks following data breaches, outside of banks controls. Ultimately, however, customers consider it banks’ responsibility to prevent social engineering fraud on their account. Examples of such social engineering methods are set out in Appendix 1.
- The survey found banks globally are seeing an increasing trend in scams. Examples of scam types are set out in Appendix 2. Fraudsters are manipulating and coercing customers into making payments to them, bypassing bank controls. The UK has introduced a *Contingent Reimbursement Model Code for Authorised Push Payment Scams* to reimburse customers in certain circumstances; and for regulators and government to deliver a sustainable solution for scam victims.
- Customers are key in the prevention and detection of fraudulent activity on their accounts, particularly to reduce scam losses. More should be done to educate customers about fraud and scams.
- Open Banking is considered a significant challenge in fraud risk by banks, with banks across the globe getting ready to open their doors to third parties to access their customer data. Questions are being raised on the reliance that can be placed on third party controls. Open Banking also presents an opportunity to gain a richer customer dataset, which can be used to prevent and detect fraudulent activity and recover fraud losses.

< 25% Over half of respondents recover less than an quarter of fraud losses. > 50% Over half of respondents globally experienced an increase in fraud value > 60% Over 60 percent of respondents globally experienced an increase in fraud volume

Typologies



Card not present (“CNP”)



Social engineering



Scams



Cyber/ online fraud

Security in a Digital World



Increasing products delivered via digital channels



Rules, machine learning, artificial intelligence & robotics



High volume of false positives

Investment versus 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

“In the context of a changing global banking landscape, where the demand for face to face banking is decreasing, volumes of digital payments are increasing and payments are being processed in seconds, fraudsters are creatively finding new ways to steal from banks and their customers. Banks need to be agile to respond to new threats and embrace new approaches and technologies to predict and prevent fraud.”

Natalie Faulkner
Global Fraud Lead,
KPMG International

© 2019 KPMG International Cooperative (“KPMG International”), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.



Themes of the survey

Fraud trends

External fraud

The survey found that in 2018, 61 percent of respondents indicated that the total volume of **external fraud** had increased and 59 percent said the value had increased.

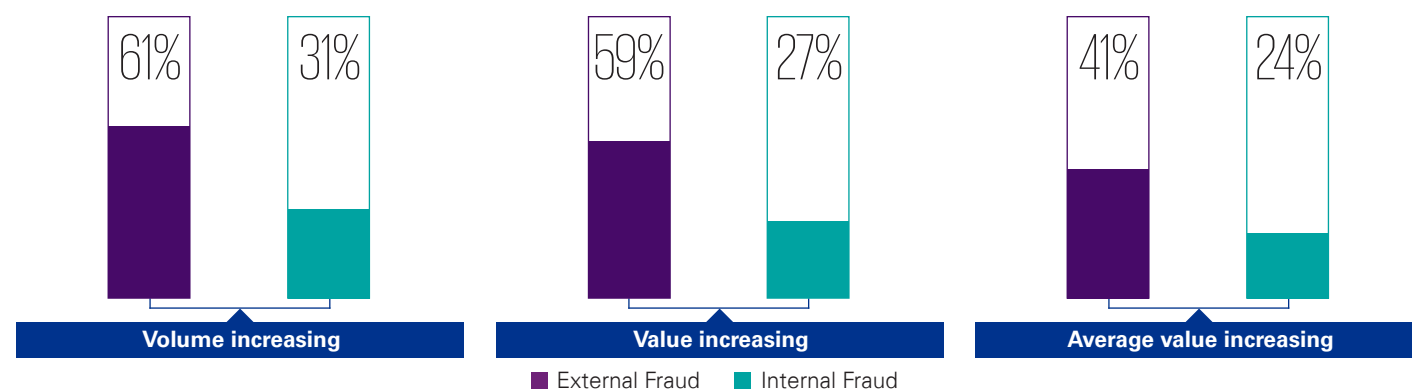
In most cases, respondents felt the average value of each fraud had stayed the same (21%) or decreased (38%). This is likely due to high volume, low value card fraud. Increasing external fraud typologies globally from 2015 to 2018 include identity theft & account takeover/impersonation fraud, cyber attack, card not present fraud and scams.

Internal (employee) fraud

In contrast, the largest proportion of respondents said that globally the total cost, average cost and volume of **internal fraud** stayed the same or decreased in 2017 and 2018. This however, may not present a complete picture of the internal threat to a financial institution, as in our experience many external fraud incidents originate with experienced criminal operatives working with internal sources who have a detailed working knowledge of bank systems, processes and controls (and any control gaps or weaknesses).

The potential harm of insider fraud can be as great, if not greater, than external fraud, given the ability of employees to exploit weaknesses in controls to target the most valuable assets of a bank. Banks should continue to take a proactive approach to detecting insider fraud.

These statistics are based on fraud detected. In our experience, fraud detection is becoming more sophisticated however there will be an element of fraud that has slipped through the gaps, yet to be detected.

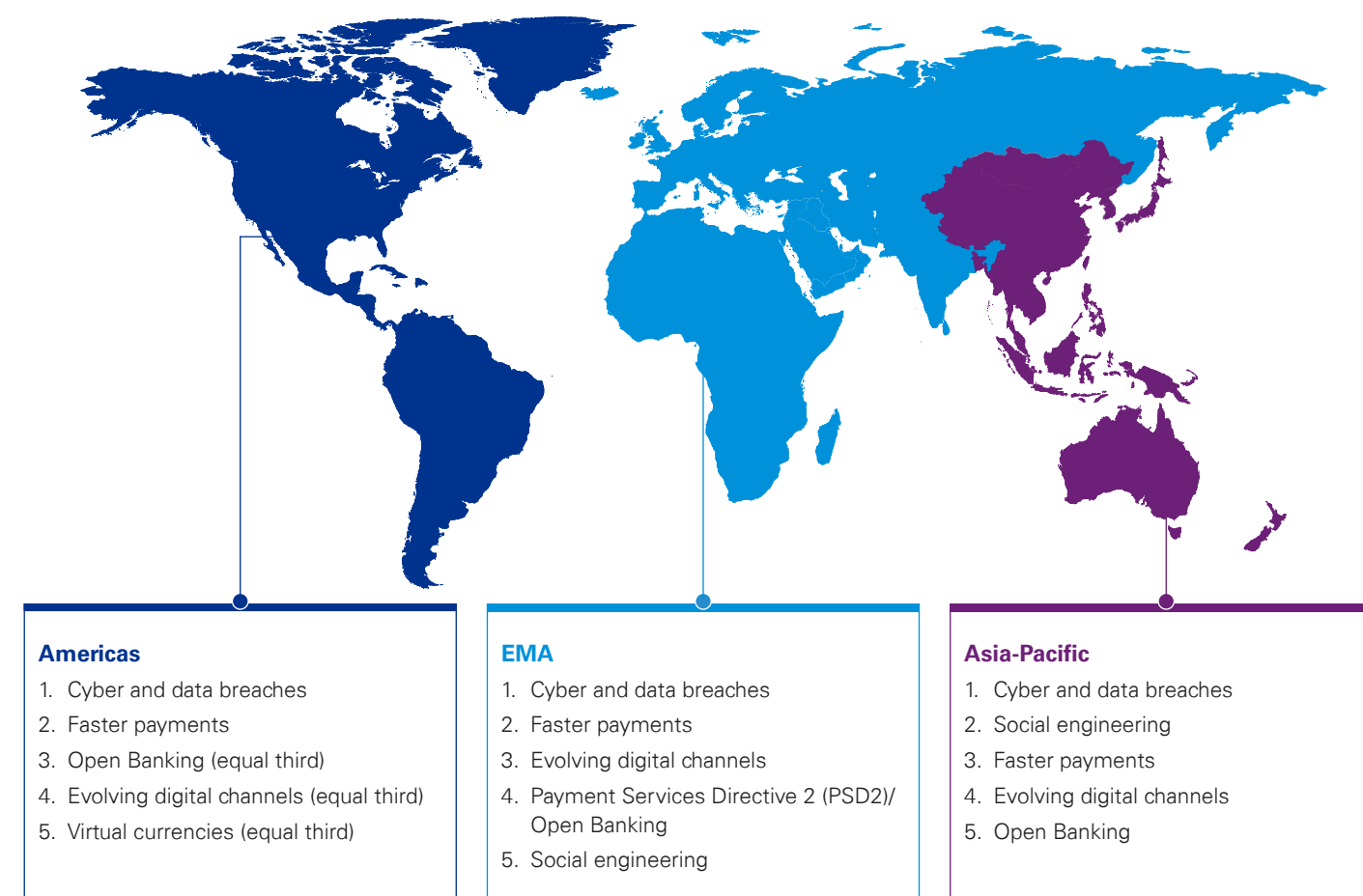


Source: Global Banking Fraud Survey, KPMG International 2019

Survey fraud typology trends by region 2017-2018 based on the most common response				
Fraud Typology	Americas	EMA	Asia-Pacific	
Scams	Increased	Increased	Increased	
Card not present	Increased	Increased	Increased	
Cyber/online fraud	Increased	Increased	Increased	
Identity theft/impersonation fraud	Increased	Increased	Increased	
Internal fraud	Increased	Increased	Stayed the same	
Data theft	Increased	Stayed the same	Increased	
Mortgage application fraud	Stayed the same	Increased	Increased	
Merchant fraud	Stayed the same	Stayed the same	Stayed the same	
Financial statement fraud	Stayed the same	Stayed the same	Stayed the same	
Rogue trading	Stayed the same	Stayed the same	Stayed the same	

Challenges facing banks today

The survey posed the question of what are the most significant challenges faced today by financial institutions in fraud risk. From a list of seven options¹, the top 5 responses by region are represented in the following chart.



Source: Global Banking Fraud Survey, KPMG International 2019

We look at these challenges in more detail below.



“Cyber related fraud risk is the most significant challenge faced by financial institutions in all three regions. In fact, the top 5 fraud risks across all three regions are in connection with the digital transformation that the world is going through. Financial institutions need a paradigm shift in their approach to mitigate fraud risks going forward. Fundamentally, financial institutions need to understand the digital transformation that is happening rapidly all around us, appreciate the evolving fraud risks arising from this rapid change and design a fraud risk management framework that is able to mitigate these fraud risks in a sustainable, effective and efficient manner. I don't think the existing “boxes” or solutions within financial institutions, while costly to maintain, are capable of dealing with the evolving fraud risks as they are too fragmented and simplistic. The new generation of fraud risk management should be able to deal with the ever evolving digital transformation, identify the unknown-unknown fraud risks, harness the benefits of technology and reduce the cost of compliance.”

Lem Chin Kok
Forensic Lead, Asia Pacific,
KPMG in Singapore



1. Cyber and data breaches

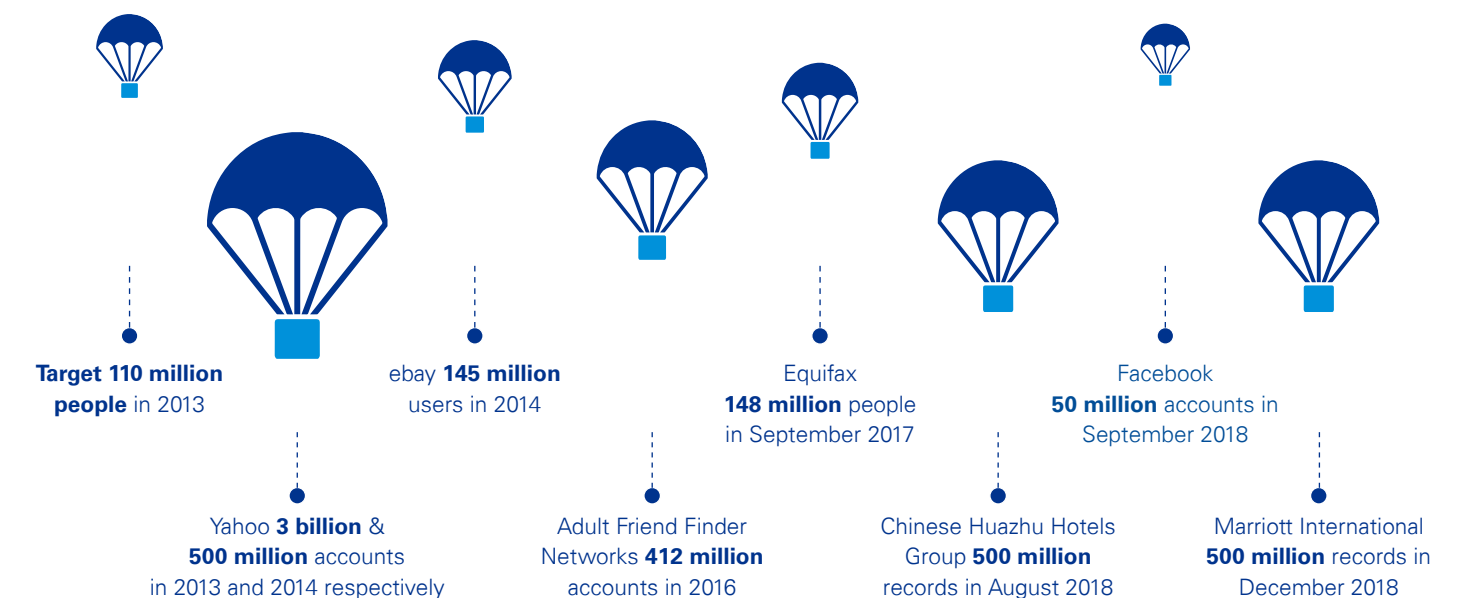
Respondents across the globe consider cyber and data breaches as the most significant challenge they face. The past few years has seen numerous high profile data breaches reported in the press, a sample of which are set out in the depiction below.

In an interconnected world, whilst a data breach may relate to one company, in one country, the data held often relates to individuals across the globe. Through these data breaches, cyber criminals are able to get hold of vast quantities of information, which can be used to facilitate identity theft, social engineering fraud and authorized push payments scams where personal data is used to gain a customer's trust, or facilitate the takeover of customer accounts.

As an example, in 2018 a major airline carrier experienced a data breach in which hackers obtained over 244,000 credit card details. The hackers charged between US\$9 and US\$50 for each card's information on the Dark Web, resulting in estimated takings of US\$12.2 million².

“Names, email addresses, passwords, social security numbers, dates of birth, credit card numbers, banking data, passport numbers, phone numbers, home addresses, driver's license numbers, medical records - they all get swept up by shadowy, amorphous hackers for fraud, identity theft”³

Customer data/records now in the public domain⁴



“As this report demonstrates, the ongoing digitization of the banking sector is certainly creating new fraud risks. But it is also spawning some amazing new solutions and opportunities for those charged with protecting the bank's customers and assets. Given the relationship between technology and fraud risk, banks may want to prioritize fraud prevention and financial crime management within their digital strategies.”

Judd Caplain
Global Head of Banking and Capital Markets,
KPMG International

2. Social engineering: A spotlight on scams

Social engineering was cited as a top 5 challenge by EMA and Asia Pacific banks surveyed.

Social engineering can result in:



Unauthorized access to customer bank accounts, where customers obtain customers' personal information that is used to gain access to their bank accounts (account takeover). Examples of some of the methods fraudsters employ to obtain customer information are set out in Appendix 1.



Authorized payments where a customer is coerced into transferring their money to an account controlled by the fraudster, on the pretext of them being a legitimate payee (also known as scams, wire fraud, authorized push payments). In this report we refer to such authorized payments as scams.

Survey respondents reported an increase in scams in each global region in 2018. From the 'Nigerian Prince' scams of old, new tricks of impersonation are being employed by fraudsters including romance, government agency/tax office, investment, lottery, business email compromise, technology support/remote access⁷ and grandparents scams, to name a few. These scams all have the same objective to obtain access to a victim's data that is then used to misappropriate the victim's funds, or persuade them to make a payment to an account controlled by the fraudster. Examples of such scams are set out in Appendix 2.

Losses to scams are exponentially growing.

In 2018, the US Federal Bureau of Investigation (FBI) reported that business email compromise scams resulted in global losses of over US\$12billion between 2013 and 2018⁸.

In Australia, the Australian Competition and Consumer Commission (ACCC) reported that almost half a billion Australian dollars was lost to scammers in 2018⁹.

This is likely just the tip of the iceberg with not all consumers knowing, or reporting that they have been scammed.

Scam victims vary. Whilst the elderly are a considerable demographic at risk, scams also impact:

- Customers who are socially isolated and lonely, such as romance scams
- Financially vulnerable such as advance fee loan scams to obtain unsecured finance, debt collection scams and investment 'too good to be true' scams
- Businesses, where a member of the finance team receives an email purporting to be the Chief Executive or Finance Officer (CEO/ CFO) requiring funds transfer, timed when they are on leave
- Youths, such as employment, vacation and lottery scams.

Banks are often blamed for failing to prevent and detect scams. From a bank's perspective, the difficulty with detecting scams is that the customer is accessing their own account, so access controls will not detect scams. Many banks now have a dedicated scams team operating in parallel with fraud teams to address this escalating risk.

Where scams are detected by banks prior to payment processing, banks are finding customers are so convinced of a scam's legitimacy, they can still be adamant they want the payment processed despite the bank informing them that a payee is fraudulent.

In most countries, there is no clear liability framework dictating who bears the cost of scams, with some banks deeming the loss as the customer's, whereas other banks assess scams on a case by case basis before determining if the bank will compensate the customer for their loss.

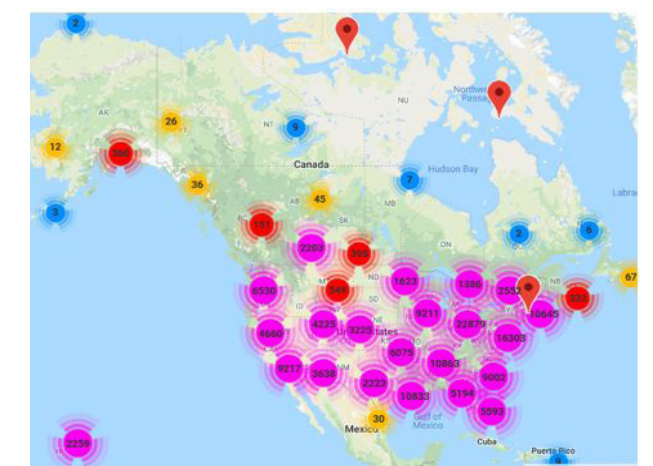
Even where the bank is not bearing the liability for scams, we are seeing this form of fraud take up significant employee time in an emotionally charged situation when customers realize they have lost significant sums.

Where the bank is bearing the liability, average losses from scams are significantly higher than card fraud.

The UK has introduced a *Contingent Reimbursement Model Code for Authorised Push Payment Scams* (the Code), to reimburse the victims of scams in any case where the bank or payment service provider is considered at fault and the customer has met the standards expected of them under the Code⁷. The Code is voluntary, and was developed in an effort to protect customers, and for regulators and government to deliver a sustainable solution. The banks who have signed up to the Code have not yet been announced, though one major retail bank has announced that it will reimburse their customers for all scams, including push payment fraud⁸. It will be interesting to see if more countries introduce similar frameworks for banks.

The following chart displays scam volumes reported by victims and potential victims in the US and Canada from 1 July 2015 to 22 April 2019.

152,595 Scams Found



Source⁹ accessed on 22 April 2019

3. Evolving digital channels and faster payment processing: The move to digital banking with less customer “face time”

Evolving digital channels was cited as a top 3 challenge by our survey respondents in the Americas and EMA.

The proportion of products and services delivered by banks through digital channels is increasing. The World Payments Report 2018 forecasts that non-cash transactions will grow compound by 12.7 percent to 2021¹⁰.

Seventy eight percent of survey respondents said more than a quarter of their products and services are delivered via digital channels. In many markets, we are seeing the emergence of neo or challenger digital banks delivering their products solely via digital channels.

With less customers holding and withdrawing cash, due to the ease of digital banking and cashless payments, customer demand for face to face banking services is diminishing. This is leading to a global trend of banks closing branches.



The UK has closed two-thirds of bank branches in the past 30 years¹¹, nearly 6,000 branches have closed in Europe¹² and in the US nearly 9,000 branches have been closed this decade¹³.

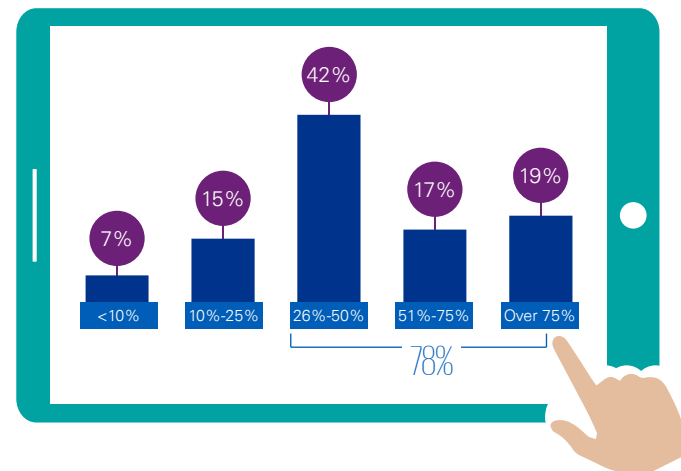
Fewer bank branches, and the increasing use of digital banking by customers requires an enhanced automated approach by banks to mitigate evolving digital fraud threats.

Further, faster payments processing can pose a challenge with less time available for banks to scrutinize transactions for fraud. Faster payments also poses the risk of reduced fraud loss recovery rates due to the velocity of payments if funds are transferred through multiple accounts in seconds and offshore.

With banks ever sensitive to the balance between fraud risk mitigation and customer experience, as seen in the survey, banks are responding via real time fraud prevention and detection tools, and imposing limits and step up authentication for higher risk transactions in an effort to mitigate the risk of increased fraud in a real time payments environment.

Authentication of alias's is also key, particularly for pull payments where fraudsters may pose as a utility or telecommunications company, for example, to request payment. The UK has responded to this risk with confirmation of payee checks when customers request fund transfers.

What proportion of your products/services are delivered via digital channels?



Source: Global Banking Fraud Survey, KPMG International 2019

- Less branches reduces the face to face interaction between banks and their customers, which is being exploited by organized criminals and fraudsters to commit fraud across borders, hacking & phishing for customer identity information to facilitate customer account takeovers.
- + More digital transactions provides a rich data set of customer digital behavior, making it easier to spot potentially fraudulent payments.

“Currently there is too much dispersion and fragmentation in fraud prevention systems within a single entity. Financial entities must evolve towards more centralized and transversal fraud management models, with the aim of identifying synergies and improving efficiency.”

Enric Olcina
Forensic Lead, Europe, Middle East and Africa,
KPMG in Spain

Banks are investing in technology to better detect fraud - so why are fraud losses increasing? We consider the challenges faced by banks in mitigating fraud, and how banks are structuring their fraud functions to respond to this changing threat as follows.

4. Open Banking

Open Banking was cited as one of the top 5 challenges facing banks in all regions. Open Banking presents a radical change to how financial institutions will operate across the globe going forward, transferring the ownership of account information from banks and financial institutions to their customers.

Customers will be able to share their details and transaction data with third parties (such as other banks, budgeting applications (apps), fintechs, telephone companies and investment platforms), through Application Programming Interfaces (APIs).

Regulators are increasingly encouraging, and in some countries mandating, that the banking industry give customers access to open banking through the development of APIs.

Open Banking is likely to impact fraud risk management in a number of ways for financial institutions:

- As with all reforms that result in faster and more convenient banking for consumers, it is likely that a higher proportion of payments will be made through digital channels, resulting in higher transaction volumes for banks reviewing account activity for fraud.
- Through open banking, banks will rely on the security of third parties to protect customer banking information accessed through APIs. Should third parties fail to provide adequate protection against fraud, customers are likely to consider the bank, rather than the apps being at fault.
- Open access to banking information across financial institutions will provide fraudsters who gain access with the ability to gather more sensitive customer data, presenting a more holistic picture of a customer's accounts to target higher positive balance 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.

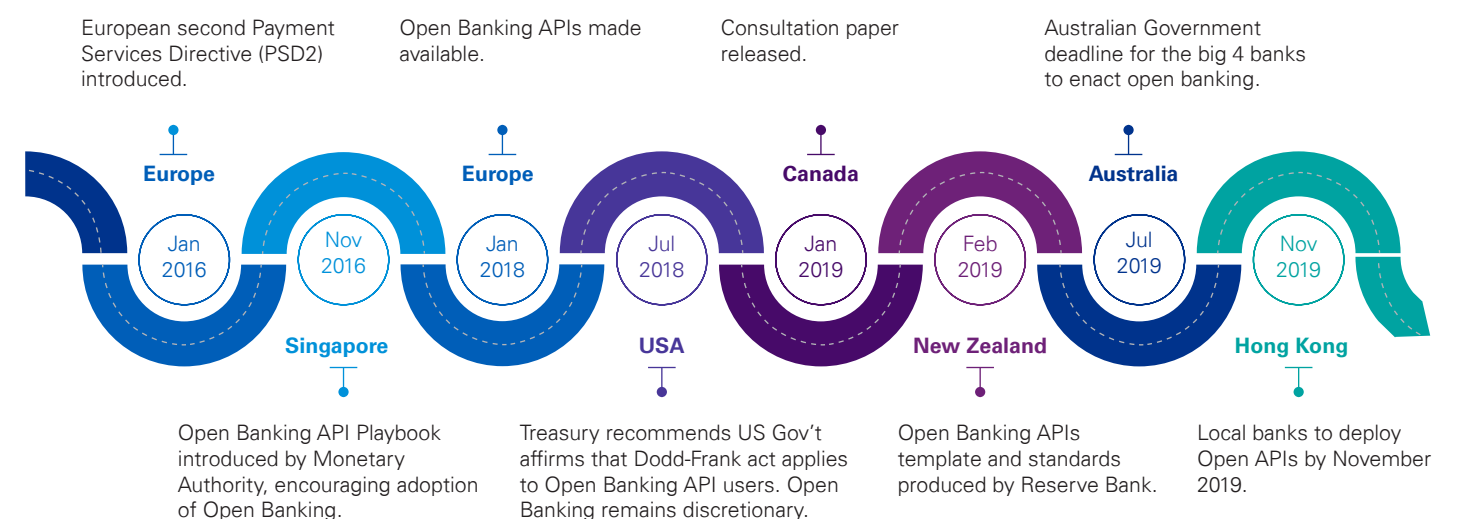
How should banks prepare?

Data security – Banking records include sensitive, confidential customer information and requires the most rigorous data security standards. Banks must ensure that APIs include robust data security controls and that third party developers are vetted before being granted access, as well as before being accredited as a service provider.

Digital identity – Open Banking relies heavily on an integrated digital identity at its foundation. Consolidation of the holistic online profile for a person, organization or electronic device will enable a secure and seamless authentication experience.

Access management – Banks will need the capability to securely and confidentially link a customer to their data. This will require a framework governing access (and revocation) rights, usage limitations and security. Much like using a social media account to login to a banking account, customers require either a standardized or customizable set of access management protocols defined for the sharing and use of data with third party service providers.

A summary Open Banking timeline across the globe

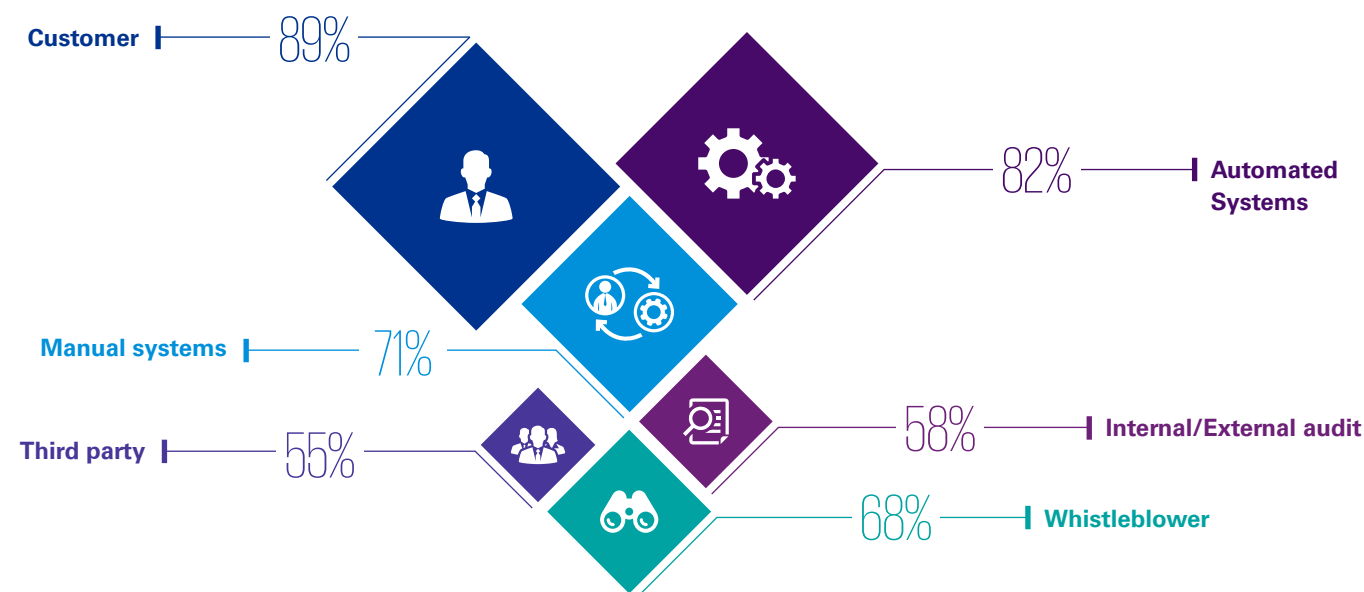


In this challenging environment, more can be done to educate customers

Customers play a key role in fraud prevention and detection, particularly in regards to scams where customers are facilitating the payment. In the survey, the majority of respondents reported customers as being a source of detection for identified fraudulent activity in 2018.

Given this finding, coupled with the low fraud recovery rate identified in the survey with over half of respondents stating recoveries are less than 25 percent of fraud losses, more can be done by banks to educate their customers to prevent and detect fraud.

How do banks identify fraudulent activity?



Source: Global Banking Fraud Survey, KPMG International 2019

Fraudsters are becoming more sophisticated. To arm customers with the skills needed to avoid falling victim to fraud, banks should educate customers to:

- Conduct timely reviews of their account activity;
 - Reverse google search images used in Romance scams;
 - Learn to spot phishing emails, text messages/SMS and phone calls;
 - Frequently change passwords;
 - Ignore pop-ups;
 - Recognize SPAM emails through spelling errors, lack of secure website information, dubious links to click and email addresses which differ from the organization purporting to be the author of the email;
 - If unsure, ask a friend or family member;
 - Remember that a genuine organization will never ask for passwords, or be concerned if you ask to end a call and phone back on a number from your records;
 - Be aware of caller ID spoofing where fraudsters mimic the phone number of the institution they are pretending to be. Caller ID spoofing has been used, for example, to appear to be a victim's friends or family phone number where the fraudster pretends that they are at the scene of an accident and their family member/friend will be left to die if they do not transfer money immediately to the caller¹⁴.
 - Remember that if the offer is too good to be true, it often is;
- Further, customer education should leverage digital and non-digital channels to cater to elderly and vulnerable customers who are often less tech savvy.

The fraud operating model

How much is fraud risk management costing you and how effective is it?

The survey asked questions to understand how banks structure their fraud risk management operations to optimize resource allocation and to inform investment decision-making across their governance, people, processes and technology.

Despite being a cost center, the total cost of fraud risk management to banks is not monitored by 52 percent of banks surveyed. This makes it an outlier within bank operations and reduces visibility to the Board and Risk Committees who make key budget, resourcing and investment decisions.

In terms of accountability for the effectiveness of fraud functions, there was a diversity of responses with respect to holding the fraud risk owner accountable for effectively preventing, detecting and responding to suspected fraud; and recovering fraud losses. Responses varied from no formal assessment to scorecards/key performance indicators, maintaining forecast losses to plan/risk appetite, business/customer satisfaction, mystery shopping and second line assurance stated.

There was a diversity in responses to how financial institutions globally structure their fraud risk management operating models.

Who owns fraud risk?



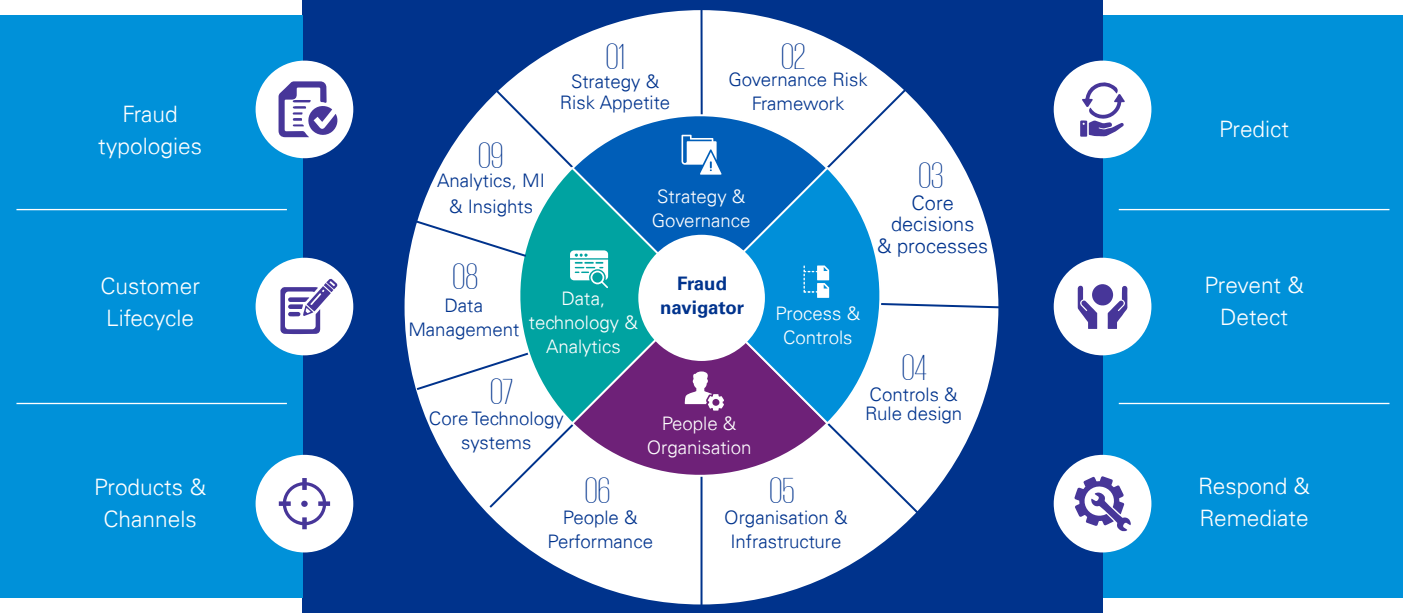
Source: Global Banking Fraud Survey, KPMG International 2019

“As fraudsters and fraud risks have become more sophisticated emanating from the shift to digital channels and tools, Regulators increasingly expect financial institutions to achieve greater consistency and integration of the First and Second lines of defense in their approach to preventing, detecting and responding to fraud risks.”

Thomas Stanton
Fraud Lead, Americas,
KPMG in the US

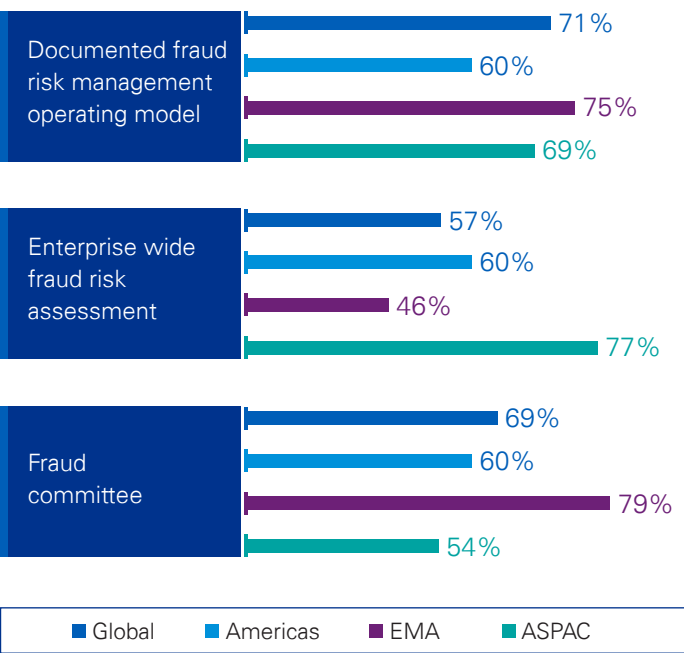
KPMG’s Fraud navigator

A well-structured fraud risk management operating model and an enterprise-wide risk assessment are important to ensure banks’ defences are robust to consistently mitigate the risk of internal and external fraud to within the bank’s fraud risk appetite.



Source: KPMG Fraud navigator 2019

The survey found not all respondents have a documented fraud risk management operating model, conduct an enterprise wide fraud risk assessment and have a fraud committee as follows:



Governance, People, Process....

The survey found differences in how financial institutions structure their fraud risk management operations, with the designated fraud risk owner found:

- 69% in the first line of defence, managed by the business units/ customer facing employees (First line);
- 31% in the second line of defence, in the group security function providing risk and compliance oversight to the business units (Second line).

Reporting lines for the fraud risk owner varied, with reporting being to the Fraud committee, Chief Risk Officer, Head of Compliance, General Counsel and Internal Audit.

Interestingly, there appears there is no one “right” model followed by banks globally to consistently structure their fraud risk management operations.

The survey found differences in who sets the bank’s fraud risk appetite, with

- * 52% Board/Risk Committee
- * 29% First line
- * 5% Second line

...and Technology

Financial institutions face a significant challenge to outpace fraudsters’ changing techniques. Banks are increasingly looking to enhance systems through enhanced transaction monitoring enabled by machine learning/artificial intelligence and biometric access management. A majority of survey respondents have invested in the following methods to predict, prevent and detect fraud attempts:

- Two or multi-factor authentication to verify a customer’s identity (requiring users to provide something they know (e.g. a password) with other factors they have (for example a text message/SMS verification code or fingerprint);
- 70 percent of banks’ surveyed have technology solutions able to risk score and make decisions in real time;
- 67 percent use physical biometrics (voice, fingerprint and facial recognition). We note that there is now a cyber crime market place for digital finger prints and cases of fraudsters recording and replicating customer voices using technology;¹⁵ and
- 63 percent use a combination of rules and machine learning embedded within their technology to facilitate fraud detection.

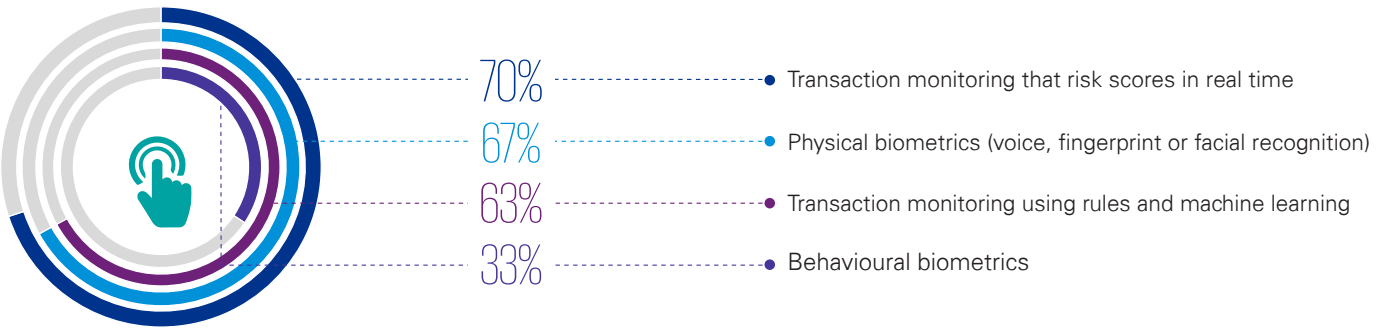
Respondents reported investments in behavioral biometrics, adverse media review technology, network analysis and Google authentication.

Despite the advances and investment in technology, 51 percent of banks’ surveyed reported a significant number of false positives resulting from their technology solutions, hampering efficiencies in fraud detection.

Ineffective systems impact fraud management information - are banks’ risks hidden in plain sight? Deficient reporting can also negatively impact the Board and Risk Committee’s ability to make appropriate resource allocation and investment decisions, with fraud investment seen to fall short of financial crime in the survey.

Furthermore, due to the size and complexity of bank operations and processes, it can take time to effect change. In contrast, fraudsters can be agile in their fraud attempts. As fraud typologies such as scams and identity theft/social engineering to facilitate account take over become more prevalent, and organized criminals share knowledge within their network across jurisdictions to overcome bank fraud detection methods, banks recognize the need to continuously hone their fraud risk management efforts to managing these risks.

Proportion of respondents who have invested in the following technology



Source: Global Banking Fraud Survey, KPMG International 2019

To continue to enhance fraud detection, survey respondents identified the need to invest in new technologies over the next three years, including:

- Transaction monitoring technology with machine learning/ artificial intelligence (AI)/robotics
- Innovations in Fintech/RegTech software automating the delivery of financial services, including automation of Know Your Customer (KYC); and
- Biometrics and a greater use of open source and social media data.

In conclusion, there are still improvement opportunities for banks to optimize their fraud operating model across governance, people, process and technology, particularly around:

- The balance between headcount and enhancements to technology;
- Optimizing resource allocation through resource planning, despite the uncertainty in time to investigate;
- Enhancing fraud detection systems, particularly to reduce false positives in systems through a feedback loop to enhance algorithms and rule sets.

Banks must plan beyond the technology to achieve results and optimum performance in their fraud operating model across governance, people, processes and technology.

What about merging fraud and financial crime compliance functions?



The significant fines being levied globally for failure to report suspected money laundering activity or associated financial crime control deficiencies are impacting investment decisions of banks to uplift financial crime ahead of fraud.

Survey results reveal over 50 percent of survey respondents globally plan to invest more in financial crime compliance (Anti-Money Laundering and Counter Terrorism Financing (AML CTF), Anti-Bribery and Corruption (ABC) and Sanctions screening) than in fraud risk management.

Our survey results found that 43 percent of respondents had integrated reporting, 40 percent had integrated governance structures, 38 percent had integrated systems and 35 percent had integrated staffing between fraud and financial crime compliance.

For 43 percent of respondents there was no integration between fraud and financial crime compliance.


The table below sets out considerations for a siloed versus an integrated model for fraud and financial crime.


 Perceived reasons to combine Fraud with Financial Crime	 Perceived reasons to silo/not combine Fraud with Financial Crime
<p>Integrated Fraud & Financial Crime teams – People & Process perspective</p> <ul style="list-style-type: none">Activities associated with Financial Crime - such as Know Your Customer (KYC) and suspicious matter reporting are also relevant to the risk of fraud. As one team with one strategy there is likely more integration to leverage intelligence regarding the same attack/incident. For example, the proceeds of crime (fraud) being passed through money mule accounts that require reporting to the Financial Crime regulator.Staff diversity of role and thinking has been stated as a benefit in integrated teams.Avoid duplication of effort or missed communications for incidents impacting both fraud and financial crime.Leverage the benefits of the significant investment going into financial crime to also benefit fraud and corruption risk management. <p>Integrated Fraud & Financial Crime teams – Technology perspective</p> <ul style="list-style-type: none">Leverage red flag/alert intelligence and dynamic customer profiling between fraud and financial crime.Cost efficiencies in using the same technology platform, with different modules and user interfaces.	<p>Siloed Fraud & Financial Crime teams</p> <ul style="list-style-type: none">Likely the main driver of siloed teams are the different regulatory reporting requirements, and specifically the significant penalties for non-reporting of financial crime suspicious matters to regulators and bribery/corruption fines and jail time in some countries (particularly by the US Securities and Exchange Commission (SEC) and the US Department of Justice (DoJ) globally). Such penalties are not levied for non-reporting of fraud.Legacy/organizational culture - “we’ve always done it this way”. <p>Siloed Fraud & Financial Crime systems</p> <ul style="list-style-type: none">Ability to pick a “best in breed” fraud system and financial crime system, potentially with a third system to identify cross purpose intelligence.Potentially a lack of awareness of appropriate solutions which can manage both risks.


Conclusion


In the context of a changing global banking landscape, where branch networks are shrinking, volumes of digital payments are increasing and payments are being processed in seconds, fraudsters are creatively finding new ways to steal from banks and their customers.


So how should banks respond?

 Our survey results show that fraudsters are shifting focus from account takeovers to scams where customers are exploited as a weak link. More needs to be done by banks to educate and protect their customers.

 Our survey reinforces that the potential harm of insider fraud can be as great, if not greater, than external fraud, given the ability of employees to exploit weaknesses in controls to target the most valuable assets of a bank. Banks should continue to take a proactive approach to detecting insider fraud.

 In the context of more countries implementing Open Banking, banks must enhance their ability to analyze big data within an open banking environment and navigate through Application Program Interfaces (API's).

 The methods used by both internal and external fraudsters continues to evolve. There is a growing need for banks to ensure the operational efficiency and effectiveness of digital fraud controls, leveraging advanced data analytics, and human expertise to predict, prevent and detect fraud. Ineffective systems impact fraud management information - are banks' risks hidden in plain sight? Deficient reporting can also negatively impact the Board and Risk Committee's ability to make appropriate resource allocation and investment decisions, with fraud investment seen to fall short of financial crime in the survey.

 Technology alone is not enough, with over half our global respondents reporting false positives hampering efficiencies in fraud detection. Banks must plan beyond the technology to achieve results and optimum performance in their fraud operating model across governance, people, processes and technology..

Fraudsters are becoming more sophisticated and can quickly change and adapt their approaches. Banks need to be agile to respond to new threats and embrace new approaches & technologies to predict and prevent fraud.

Appendix 1

Examples of social engineering methods

Phishing/ Spoofing: A phishing attack is where a scammer sends an e-mail pretending to be someone or something they are not in order to obtain personal information from their victim. Phishing commonly involves a user clicking a link and entering their password, after which the scammer will have sufficient information to obtain access to the victim’s account or mailbox. On average, 4% of the targets of any given phishing campaign will click on the link.

Spear Phishing: Spear phishing refers to phishing attempts where the scammer uses open source information to craft e-mails that are highly customised to further encourage the victim to click on a link in their e-mail. For instance, a scammer may identify through social media that a victim is expecting a parcel, and will craft a phishing e-mail appearing to be from the delivery service, with a message regarding that parcel with a fake link to track the delivery.

Pretexting: Pretexting is a form of social engineering in which the attacker fabricates a scenario, a convincing pretext, for why they require information from the victim. Typically, scammers will impersonate people in a position of authority, such as the tax authorities, or a bank, and request information from their target in order to confirm their identity.

Baiting: Baiting is a social engineering attack designed to manipulate the victim through their curiosity. The scammer will offer the victim a good of some kind (such as a software update, a prize or leaving a USB in a public place for a victim to plug into their computer), which once opened by the victim will compromise the victim’s computer to install malicious software.

Quid Pro Quo: This is a variant of baiting where the scammer will promise a service or benefit following the execution of a specific action. For instance, a hacker may impersonate an IT security specialist, offering a software upgrade, providing the victim disable their antivirus software first, thereby installing malicious software unimpeded onto the computer.

Appendix 2

Scam Typologies

Average amount lost per scam			
Investment	\$8,648	Fake invoice	\$441
Romance	\$6,003	Credit repair/debt relief	\$388
Moving	\$3,993	Online purchase	\$365
Cryptocurrency*	\$3,147	Fake check/money order	\$341
Home improvement	\$2,895	Tech support	\$255
Nigerian/Foreign money exchange	\$2,133	Credit card	\$231
Business email compromise	\$1,717	Government grant	\$218
Family/friend emergency	\$1,219	Health care/medical/medicare	\$170
Counterfeit product	\$1,210	Scholarship	\$155
Travel/vacation	\$887	Utility	\$106
Advance fee loan	\$716	Debt collection	\$98
Charity	\$708	Yellow pages/directory	\$91
Identity theft	\$683	Phishing	\$44
Rental	\$662	Tax collection	\$31
Employment	\$598	Other	\$746
Sweepstakes/lottery/prize	\$547		

* Denotes a category first tracked in 2018

Source: BBB Scam Tracker, 2015 to December 2018
The average losses in the Americas, by scam typology.

Investment scams: Investment scams present the victim with an unbeatable opportunity, often to make guaranteed high returns, should they invest their money. Victims are often contacted by phone or e-mail by fraudsters claiming to offer genuine investment advice.

Romance scams: Dating and romance scams take advantage of people looking for love, creating fake profiles on dating websites or social media sites pretending to be a potential romantic partner. Following an often protracted online courtship, the fraudster will ask for money, gifts or personal information. Scams often play on the victims emotional triggers, for instance asking for money to pay for ‘family medical bills’ or for flights so that they can visit the victim. Fraudsters may also ask for intimate photos which they will then use to blackmail the victim.

Nigerian Prince scam: The ‘Nigerian Prince’ scam, one of the longest running scams, in which the victim is contacted by someone claiming to be from overseas who claims to be very wealthy and/or royalty requesting assistance to move money out of their country for the opportunity to share in the millions of dollars, are still remarkable prevalent and effective. Requests are made for the victim to pay taxes, bribes to government officials and legal fees with a promise all expenses will be reimbursed when the funds are out of the country. Once in possession of the payment, or bank details, the ‘Prince’ will disappear, often with the contents of the victim’s bank account.

Business E-mail Compromise (BEC): A common form of e-mail fraud, BEC targets individuals with access to company banking facilities and uses social engineering to trick them into making payments to fraudsters. Frequently, the fraudster will pretend to be the CEO of the company, requesting an urgent payment that bypasses usual controls. The FBI’s Internet Crime Complaints Centre (IC3) published in June 2018 BEC as a US\$12 billion scam.

Family/ friend emergency: Often targeted to the elderly and playing on poor hearing, the fraudster will pretend to be the victim’s grandchild. The ‘grandchild’ will claim to be in trouble needing money (for instance pretending to be in jail, in legal trouble or in debt). Victims are often told that they are the only person the grandchild trusts and not to tell anyone else. Scammers will use details from social media to make their story sound more believable and obscure their voices by feigning crying.

Lottery scams: Lottery scammers contact victims informing them that they have won the lottery or a prize draw that they had never actually entered. Victims will be asked to pay an up front fee to release or deliver their gift or monies. They may also be asked to call a high rate telephone number to claim the prize. Often fraudsters will use the names of real competitions so that if the victim researches the scam it appears legitimate.

Tech Support/Remote Access Scams: Tech support/ Remote access scams convince the victim that there is a computer or internet problem and that new software is required to fix the problem. The victim will receive a call, e-mail or a computer pop-up informing them that there are issues with their internet connection or computer and direct the victim to contact the fraudster to get it fixed. Scammers may cite common problems such as internet speed as evidence of the problem. They will then request the victim provide them with remote access to ‘find out what the problem is’. Once the fraudster has access to the victim’s computer they harvest their data, access their Bank accounts and often make payments to themselves.

Government agency scams: In a government agency scams, fraudsters contact victims by phone, text or e-mail pretending to be from a judiciary body or the tax office. In some instances the fraudster will ask for an urgent payment to settle a debt such as an overdue parking fine or tax payment. The fraudster may threaten that non-payment will result in the payment increasing or jail time.

Appendix 3

Sources

2013 Target: 110 million. Based on figure quoted in report by The Huffington Post, “Target Hacked: Retailer Confirms ‘Unauthorised Access’ Of Credit Card Data” (19 December 2013). Available at https://www.huffpost.com/entry/target-hacked-customer-credit-card-data-accessed_n_4471672

2013 Yahoo: 3 billion. Based on figure quoted in report by The New York Times, “All 3 Billion Yahoo Accounts Were Affected by 2013 Attack” (Nicole Perlroth, 3 October 2017). Available at: <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>

2014 Yahoo: 500 million. Based on figure quoted in report by The Washington Post, “Yahoo confirms data breach affecting at least 500 million accounts” (Hayley Tsukayama, Craig Timberg & Brian Fung, 22 September 2016). Available at: <https://www.washingtonpost.com/news/the-switch/wp/2016/09/22/report-yahoo-to-confirm-data-breach-affecting-hundreds-of-millions-of-accounts/>

2014 Ebay: 145 Million. Based on figure quoted in report by The Washington Post, “eBay asks 145 million users to change passwords after data breach” (Andrea Peterson, 21 May 2014). Available at: <https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/>

2016 Adult Friend Finder: 412 million. Based on figure quoted in report by The Verge, “Over 300 million AdultFriendFinder accounts have been exposed in massive breach” (Andrew Liptak, 13 November 2016). Available at: <https://www.theverge.com/2016/11/13/13615750/412-million-adultfriendfinder-accounts-exposed-breach>

September 2017 Equifax: 148 million American Consumers. Based on figure produced by U.S. House of Representatives Committee on Oversight and Government Reform, The Equifax Data Breach Report (December 2018) p2. Available at: <https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>

August 2018 Chinese Huazhu Hotels Group: 500 million records. Based on figures quoted in report by China Daily, “Huazhu Hotels Group investigates alleged info leak” (29 August Adata (including name and mobile numbers), 130 million check-in records (including name and address) and 240 million hotel stay records (including credit card numbers and check in and out dates).

September 2018 Facebook: 50 million accounts. Based on figures quoted in report by The Guardian, “Facebook says nearly 50m users compromised in huge security breach” (Julia Carrie Wong, 29 September 2018). Available at: <https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach>

2018 Marriott International: 500 million records. Based on figures quoted in report by The New York Times, “Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing” (David E. Sanger et al, 11 December 2018). Available at: <https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html>

The Daily Mail, “Russian hackers made £9.4m from British Airways data breach with customers’ credit card details put on sale for as little as £6.94, experts say” (Sami Quadri, 14 November 2018). Credit card details available for sale were from customers through Europe and from Mexico, Brazil and China including others. Available at: <https://www.dailymail.co.uk/news/article-6387001/Russian-hackers-9-4m-British-Airways-data-breach.html>

Wired, “The Wired Guide to Data Breaches” (Lily Hay Newman, 12 July 2018). Available at: <https://www.wired.com/story/wired-guide-to-data-breaches/>

FBI Public Service Announcement, “Business E-Mail Compromise: The 12 Billion Dollar Scam” (12 July 2018). Report states that 78,617 incidents of business e-mail compromise scams occurred between October 2013 and May 2018 resulting in global losses of US\$12,536,948,299. Business e-mail compromise scams are defined as “when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorised transfers of funds”. Available at: <https://www.ic3.gov/media/2018/180712.aspx>

Australian Competition and Consumer Commission, Targeting Scams Report (May 2019). \$489 billion in losses reported to the ACCC from over 378,000 scam reports. Available at <https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2018>

Authorised Push Payment Scams Steering Group 28 February 2019 Press release, and attached copy of the Code. The Code states that the customer may not be refunded if the customer “ignored effective warnings”, “did not take appropriate actions” or where the behaved in a way that was “grossly negligent.” The Code comes into force on 28 May 2019, signatories have not yet been announced. Available at: <https://appcrmsteeringgroup.uk/app-scams-steering-g>

¹ Faster payments, Cyber and data breaches, Payment Services Directive 2/ Open banking, Virtual currencies, Evolving digital channels, Social engineering, Criminal use of artificial intelligence.

² The Daily Mail, “Russian hackers made £9.4m from British Airways data breach with customers’ credit card details put on sale for as little as £6.94, experts say” (Sami Quadri, 14 November 2018). Credit card details available for sale were from customers through Europe and from Mexico, Brazil and China including others. Available at: <https://www.dailymail.co.uk/news/article-6387001/Russian-hackers-9-4m-British-Airways-data-breach.html>

³ Wired, “The Wired Guide to Data Breaches” (Lily Hay Newman, 12 July 2018). Available at: <https://www.wired.com/story/wired-guide-to-data-breaches/>

⁴ 2013 Target: 110 million. Based on figure quoted in report by The Huffington Post, “Target Hacked: Retailer Confirms ‘Unauthorised Access’ Of Credit Card Data” (19 December 2013). Available at https://www.huffpost.com/entry/target-hacked-customer-credit-card-data-accessed_n_4471672

2013 Yahoo: 3 billion. Based on figure quoted in report by The New York Times, “All 3 Billion Yahoo Accounts Were Affected by 2013 Attack” (Nicole Perlroth, 3 October 2017). Available at: <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>

2014 Yahoo: 500 million. Based on figure quoted in report by The Washington Post, “Yahoo confirms data breach affecting at least 500 million accounts” (Hayley Tsukayama, Craig Timberg & Brian Fung, 22 September 2016). Available at: <https://www.washingtonpost.com/news/the-switch/wp/2016/09/22/report-yahoo-to-confirm-data-breach-affecting-hundreds-of-millions-of-accounts/>

2014 Ebay: 145 Million. Based on figure quoted in report by The Washington Post, “eBay asks 145 million users to change passwords after data breach” (Andrea Peterson, 21 May 2014). Available at: <https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/>

2016 Adult Friend Finder: 412 million. Based on figure quoted in report by The Verge, “Over 300 million AdultFriendFinder accounts have been exposed in massive breach” (Andrew Liptak, 13 November 2016). Available at: <https://www.theverge.com/2016/11/13/13615750/412-million-adultfriendfinder-accounts-exposed-breach>

September 2017 Equifax: 148 million American Consumers. Based on figure produced by U.S. House of Representatives Committee on Oversight and Government Reform, The Equifax Data Breach Report (December 2018) p2. Available at: <https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>

August 2018 Chinese Huazhu Hotels Group: 500 million records. Based on figures quoted in report by China Daily, “Huazhu Hotels Group investigates alleged info leak” (29 August 2018). Available at: <http://www.chinadaily.com.cn/a/201808/29/WS5b86473da310add14f38871b.html>. Unauthorized access to Huazhu Hotels Group 123 million pieces of registration data (including name and mobile numbers), 130 million check-in records (including name and address) and 240 million hotel stay records (including credit card numbers and check in and out dates).

September 2018 Facebook: 50 million accounts. Based on figures quoted in report by The Guardian, “Facebook says nearly 50m users compromised in huge security breach” (Julia Carrie Wong, 29 September 2018). Available at: <https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach>

2018 Marriott International: 500 million records. Based on figures quoted in report by The New York Times, “Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing” (David E. Sanger et al, 11 December 2018). Available at: <https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html>

⁵ FBI Public Service Announcement, “Business E-Mail Compromise: The 12 Billion Dollar Scam” (12 July 2018). Report states that 78,617 incidents of business e-mail compromise scams occurred

between October 2013 and May 2018 resulting in global losses of US\$12,536,948,299. Business e-mail compromise scams are defined as “when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorised transfers of funds”. Available at: <https://www.ic3.gov/media/2018/180712.aspx>

⁶ Australian Competition and Consumer Commission, Targeting Scams Report (May 2019). \$489 billion in losses reported to the ACCC from over 378,000 scam reports. Available at <https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2018>

⁷ Authorised Push Payment Scams Steering Group 28 February 2019 Press release, and attached copy of the Code. The Code states that the customer may not be refunded if the customer “ignored effective warnings”, “did not take appropriate actions” or where the behaved in a way that was “grossly negligent.” The Code comes into force on 28 May 2019, signatories have not yet been announced. Available at: <https://appcrmsteeringgroup.uk/app-scams-steering-group-agrees-voluntary-code/>.

⁸ The Independent, “TSB becomes first bank to offer ‘refund guarantee’ to all fraud victims” (Ben Chapman, 16 April 2019). Available at: <https://www.independent.co.uk/news/business/news/tsb-bank-fraud-guarantee-refund-scams-a8870781.html>

⁹ BBB Scam Tracker, reporting US and Canadian victim and potential victim accounts from 1 July 2015 to 22 April 2019. Available at: <https://www.bbb.org/scamtracker/us/>

¹⁰ World Payments Report 2018, p6. Available at <https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf>

¹¹ The Financial Times, “UK has lost two-thirds of bank branches in 30 years” (Emma Agyemang, 16 November 2018). Available at: <https://www.msn.com/en-gb/money/news/uk-has-lost-two-thirds-of-bank-branches-in-30-years/ar-BBPL1Z7>

¹² The European Banking Federation, 2018 Facts & Figures (11 September 2018). Available at: <https://www.ebf.eu/ebf-media-centre/banking-in-europe-ebf-publishes-2018-facts-figures/>)

¹³ The Wall Street Journal, “Thousands of Bank Branches are Closing, Just Not at These Banks” (Allison Prang, 15 June 2018). Available at: <https://www.wsj.com/articles/the-bank-branch-is-dying-just-not-at-these-banks-1529055000>

¹⁴ CNBC.com, “You think it’s your friend calling, but it’s actually this growing phone scam” (Annie Nova, 12 June 2018). Available at: <https://www.cnbc.com/2018/06/12/you-think-its-your-friend-calling-but-its-actually-this-growing-phone-scam.html>

¹⁵ <https://www.zdnet.com/article/cybercrime-market-selling-full-digital-fingerprints-of-over-60000-users/>



Contacts

David Hicks

Global Forensic Leader
KPMG International
T: +44 20 76942915
E: David.Hicks@KPMG.co.uk

Judd Caplain

Global Head of Banking and Capital Markets
KPMG International
T: +1 212 872 6802
E: jcaplain@kpmg.com

Natalie Faulkner

Global Fraud Lead
KPMG International
T: +61 2 9335 7716
E: nfaulkner1@kpmg.com.au

Enric Olcina

Fraud Lead, Europe, Middle East and Africa
KPMG in Spain
T: +34 93 2532 985
E: eolcina@kpmg.es

Thomas Stanton

Forensic Lead, Americas
KPMG in the US
T: +1 212 872 7758
E: tstanton@kpmg.com

Lem Chin Kok

Forensic Lead, Asia Pacific
KPMG in Singapore
T: +65 6213 2495
E: clem@kpmg.com.sg

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2019 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Throughout this document, "we" "KPMG", "us" and "our" refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Designed by: KGS

Publication date: May 2019