Why Fraud Management Needs a Digital and Centralized Strategy

www.hexaware.com

Table of Contents

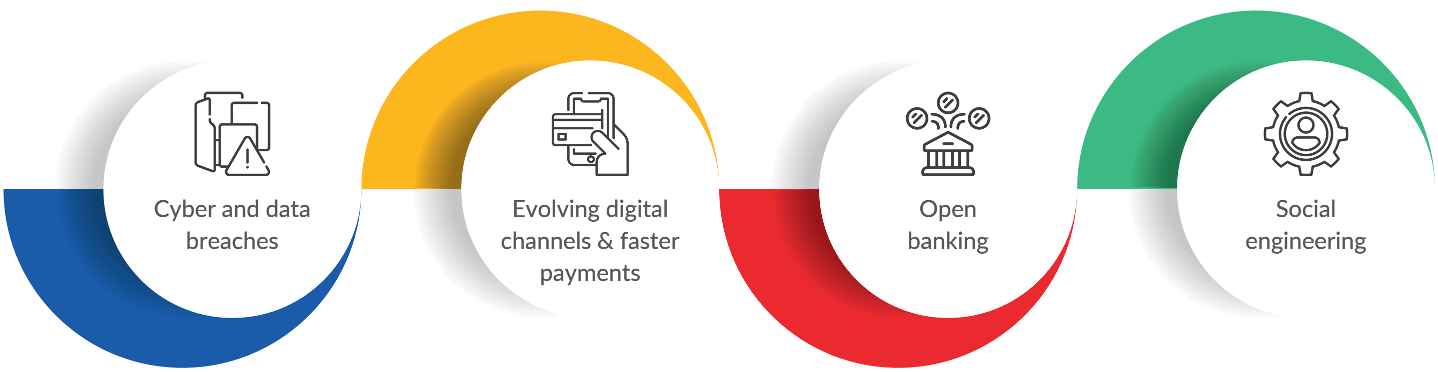
> *“For fraud groups that have not transformed their technologies and operations, this (COVID-19) crisis has highlighted the need to view fraud as a strategic imperative, not just a bottom-line expense."*
>
> — Steven D'Alfonso, research director, IDC Financial Insights[1]

Fraud incidents are evolving with digital banking

We have seen the rapid evolution of digital banking, especially in the last five years. From branch to digital-only banking, the industry has witnessed a dramatic change in how customers access banking services. More people across age groups and geographies are exploring and embracing digital banking in different forms like online account opening, P2P payments, mobile payments, and digital wallets. Among the demographic cohorts, the millennials and the Gen-Zers have been the biggest consumers of digital banking. The rise of challenger banks, also known as neobanks that reside entirely in the online/digital space have disrupted the way in which banking is done. They are also pushing the incumbent banks to evolve their digital models.

While digital banking has contributed to making banking transactions convenient and easy for customers, it has also led to a new breed of digital banking frauds. These include phishing, synthetic identities, stolen identities, business email compromise, and account takeover.

KPMG’s Global Banking Survey[2] of 43 retail banks conducted between November 2018 and February 2019 revealed that the top challenges included:



The survey revealed:

- More than 50% of respondents experienced an increase in fraud value
- More than 60% of respondents experienced an increase in fraud volume
- More than 50% of respondents stated fraud recoveries were less than 25% of fraud losses
- There was an increase of 61% in volume and 59% in value in external fraud
- There was an increase of 31% in volume and 27% in value in internal fraud

The survey also discovered that:

- The cost of fraud was increasing faster than fraud risk management spend
- Despite being a cost center, the total cost of fraud risk management was not monitored by 52% of the banks surveyed

Fraudsters are exploiting the pandemic

Today, banking frauds have found a bigger canvas in the pandemic. Social distancing and safety norms have made digital banking the go-to option, compelling more customers to use digital wallets, make mobile payments, and access internet banking. People are also spending more time online to work, to socialize, and to look up for information and updates related to the pandemic. All this creates greater opportunities for fraudsters to find new ways to manipulate them.

- Standard Chartered reported[3] that in March and April 2020, they experienced several instances of unauthorized payment instructions purportedly from FI clients; clients sending payments for PPE and related materials to fraudulent sellers, and identification of mule accounts used to receive fraudulently obtained funds.
- About £2m has been lost to coronavirus-related fraud in the UK and more than 70,000 "malicious" websites have sprung up since the global pandemic was declared.[4]
- Between January and April 2020, the Federal Trade Commission (FTC) had received 18,235 reports related to COVID-19, and people reported losing $13.44 million to fraud.[5]

Evolving fraud typologies

	Digital banking frauds	
Banking frauds	**Evolving digital models & open banking**	**Greater digital fraud opportunities due to the pandemic**
Check frauds	Phishing	Fraudulent websites with fake COVID-19 domains carrying malware
Frauds related to credit and debit cards	Synthetic identities	Charity scams (soliciting donations)
Wire transfer frauds	Stolen identities	Fake fines and warnings (breaking lockdown rules; not wearing a mask, etc.)
ATM frauds	Business email compromise	Social engineering: fundraising scams publicized on social media
Check frauds	Account takeover (ATO)	COVID-19-themed phishing emails
	Mobile app scams	

The digital transformation journey in the last five years had already made banks vulnerable to greater incidents of fraud. COVID-19 has now dramatically increased the digital opportunity for manipulation.

The different facets of digital fraud

Phishing: Where someone posing as a recognized institution will typically send an email or text message to lure a customer into divulging sensitive data like username, password, PIN, and other personally identifiable information. Phishing emails will have hyperlinks or attachments designed to attack the customer's computer or device.

Synthetic identities: Where the fraudsters create a whole new fake identity by adding some real data from different sources.
Stolen identities: Where a real person's identity is stolen with information such as name, credit card details, and social security number to commit fraud.

Business email compromise: In this, fraudsters typically target company employees by sending them an email message that looks like it has been sent from a legitimate address, company, supplier, etc. The email will have a minor variation that will go undetected and trick the victim into divulging confidential information or clicking on a malware file.

Account Takeover: Here, criminals gain access to the customer account details and leverage the information to make purchases or withdraw funds.

COVID-19-related scams: There has been a dramatic increase in scams designed to take advantage of pandemic-induced fears and vulnerabilities in people. These scams range from fraudulent websites with malware; charity and fund-raising scams that solicit donations that appeal to the humanitarian side of people; warning scams that exploit fear among people, forcing them open an email or click on a link by making them believe that they have violated a COVID-19 protocol.

Risks

The evolving nature of frauds is increasing the risk for banks at three levels:

Reputational: Negative publicity and consequently negative public opinion can be highly damaging to a bank's reputation. It can lead to panic, withdrawal of money, loss of customers, and also impact the nation's economy.

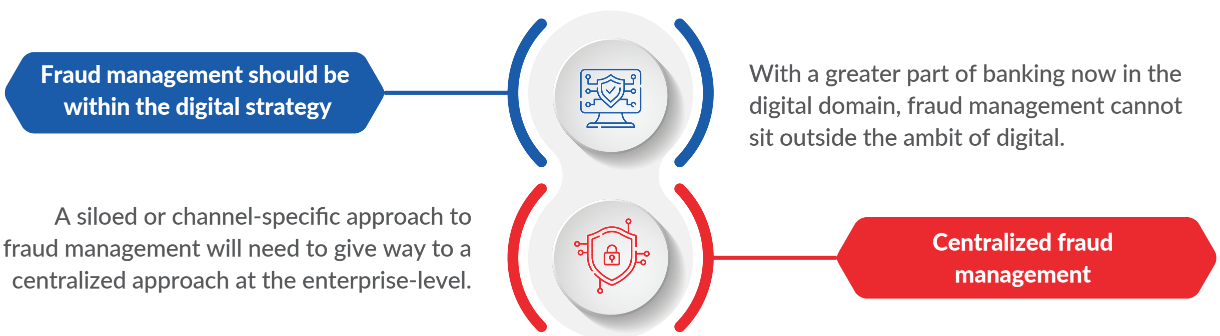
Regulatory: Regulators expect banks to conduct forensic audits and report irregularities immediately. The risk of breaking regulatory laws like data privacy or a delay in detecting and reporting frauds swiftly can invite action and hefty fines from authorities.

Transactional: Millions of digital banking transactions every day can increase the risk of scams and frauds for customers.

Fraud management strategy

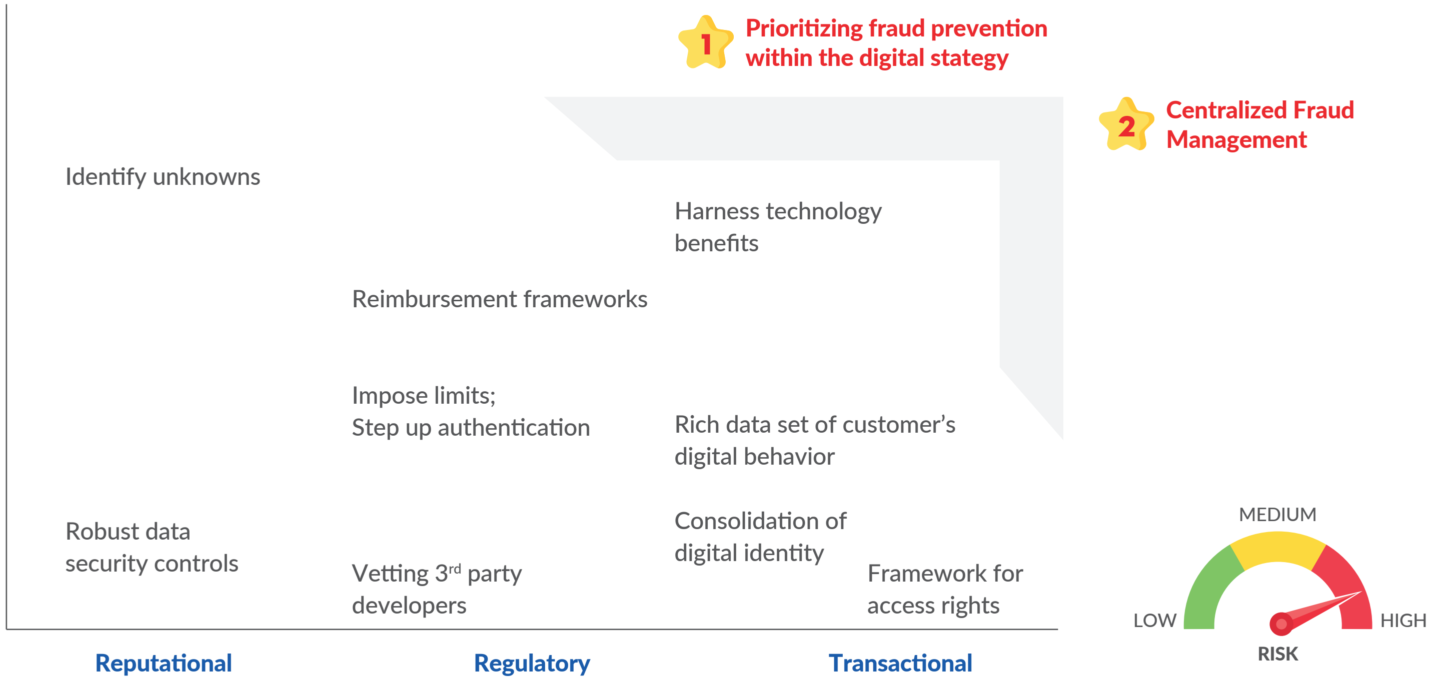
Digital fraud is now large-scale and industrialized. Therefore, any approach to fraud management that is outside the digital strategy will make it obsolete. Every time there is a digital shift, banks will need to go through the cycle of discover, design, and deploy, to tackle evolving frauds. The challenge will only get exacerbated when banking institutions attempt to tackle the fraud within its channel or silo. This reduces the visibility at the enterprise level on the nature, network, volume, and value of the fraud. It also makes it difficult to have a centralized strategy and allocate budgets for fraud detection and prevention.

To mitigate losses and meet revenue targets, fraud management will require a two-pronged approach:



Effective fraud management cannot sit outside the digital strategy and cannot have a siloed approach

A centralized and digital approach will help to control risks and counter fraud across reputational, regulatory and transactional levels



A blueprint for effective fraud management

An effective fraud management strategy should have a holistic approach to minimize risks, starting with governance and assessment, to prevention, detection, and response.

Governance

- *Fraud control strategy blueprint*
- *Anti-fraud policy definition*
- *Control activities design*
- *Roles & Responsibilities formalization*
- *Practice definition*

Assessment

- *Key areas customization*
- *Fraud types prioritization*
- *Vulnerabilities assessment*
- *Key business unit assessment*
- *Fraud scheme level assessment*

Prevention

- *Fraud awareness management*
- *Employee training*
- *Fraud prediction management*
- *Fraud prevention measurement*
- *Fraud prevention techniques*

Detection

- *Transaction fraud detection*
- *Application fraud detection*
- *Access fraud detection*
- *Fraud anomaly detection*
- *Benchmarking fraud helplines/hotlines*

Response

- *Fraud investigation*
- *Protocols establishment*
- *Resource identification*
- *Fraud association management*
- *Fraud to information association*
- *Fraud to risk association*
- *Fraud claims handling*
- *Fraud estimation*
- *Fraud claim validation*
- *Liability determination*
- *Fraud claim resolution*

Partnering with the right systems integrator to combat fraud

Over the years, systems integration has evolved into a strategic capability, combining expert consulting with technology integration of both home-grown tools as well as industry-leading technology solutions. Given the risk and impact of fraud, the role of a systems integrator cannot be over-stated. Frauds are increasingly complex, as well as evolving continuously. It is therefore crucial for banks to partner with an expert systems integrator (SI) who will leverage an integrated and all-inclusive approach to detect and prevent fraud.

Your systems integrator should have an all-inclusive approach to fraud management

An all inclusive approach

- Governance
- Assessment
- Prevention
- Detection
- Response
- Fraud Investigation
- Fraud Association
- Fraud Claims

Solution Blocks

- Consulting Toolkits
- Predictive Fraud Models
- Real-time Detection
- Alerts Management
- Enterprise Case Management
- Next-Gen Authentication
- Centralized Data Repository

Technology

- Rule-based Engine
- Supervised Machine Learning
- Unsupervised Machine Learning
- Anomaly Detection

Internal Structured Data
Relationship — Banking, Loans, Cards, Investments

External Unstructured Data
Social Media, Call Center, Credit Bureau, Watch List

Transaction Data
Across channels — Web Banking, ATM, POS, Mobile Banking App

Hexaware's fraud management solutions

Hexaware combines its deep domain experience with sophisticated technology capabilities and fintech partnerships to offer an integrated, all-inclusive approach to fraud management.

Our competencies include:

- **Consulting services:** to help you assess the gaps in your future state and to prepare you to address the gaps before fraud can occur.
- **Domain expertise:** our solid experience in banking will help to keep banks ahead of the curve for solution conceptualization.
- **Technology capability:** we enjoy deep expertise in a wide variety of technologies; being vendor agnostic, we are also able to deploy a solution that is best suited to your institution.
- **Fintech partnerships:** we provide access to a sophisticated fintech eco-system that will help banks to leverage pre-built fintech solution components for rapid implementation.

To know more, write to *marketing@hexaware.com*.

References

[1] Steven D'Alfonso quote
Retrieved from: *https://www.idc.com/getdoc.jsp?containerId=US46633120*

[2] KPMG's Global Banking Survey
Retrieved from: *https://home.kpmg/xx/en/home/insights/2019/05/the-multi-faceted-threat-of-fraud-are-banks-up-to-the-challenge-fs.html*

[3] Standard Chartered report on unauthorized payments
Retrieved from: *https://www.sc.com/en/feature/why-increasing-awareness-and-collaboration-are-key-to-tackling-covid-19-fraud/*

[4] Coronavirus-related fraud in the UK
Retrieved from: *https://www.bbc.com/news/uk-england-52310804*

[5] Covid-19 scam reports by the Federal Trade Commission (FTC)
Retrieved from: *https://www.consumer.ftc.gov/blog/2020/04/covid-19-scam-reports-numbers*

About Hexaware

Hexaware is the fastest growing next-generation provider of IT, BPO and Consulting services. Our focus lies on taking a leadership position in helping our clients attain customer intimacy as their competitive advantage. Our digital offerings have helped our clients achieve operational excellence and customer delight. We are now on a journey of metamorphosing the experiences of our customer's customers by leveraging our industry-leading delivery and execution model, built around the strategy— 'AUTOMATE EVERYTHING™, CLOUDIFY EVERYTHING™, TRANSFORM CUSTOMER EXPERIENCES™.' Hexaware services customers in over two dozen languages, from every major time zone and every major regulatory zone. Our goal is to be the first IT services company in the world to have a 50% digital workforce. Learn more about Hexaware at http://www.hexaware.com

NA Headquarters
Metro 101, Suite 600,101
Wood Avenue South, Iselin,
New Jersey - 08830
Tel: +001-609-409-6950
Fax: +001-609-409-6910

India Headquarters
152, Sector – 3
Millennium Business Park
'A' Block, TTC Industrial Area
Mahape, Navi Mumbai – 400 710
Tel : +91-22-67919595
Fax : +91-22-67919500

EU Headquarters
Level 19, 40 Bank Street,
Canary Wharf,
London - E14 5NR
Tel: +44-020-77154100
Fax: +44-020-77154101

APAC Headquarters
Hexaware Technologies
Asia Pacific Pte Ltd, #09-01,
One Finlayson Green,
1 Finlayson Green
Singapore-049246
Tel : +65-63253020
Fax : +65-6222728

Australia Headquarters
Level 3, 80 Mount St
North Sydney
NSW 2060
Australia
Tel : +61 2 9089 8959
Fax : +61 2 9089 8989