GATE ONE

Banking fraud

STAYING A STEP AHEAD

Staying a step ahead

The banking sector is no stranger to forced evolution. Digital banking services are winning market share from high street banks, driving them to control costs and innovate services. Equally, organised crime and fraud are now a significant evolutionary force. As a result the sector is now dealing with two opposing priorities: protecting its customers from increasingly sophisticated fraud, while providing a relevant customer experience.

COVID-19 has resulted in an accelerated shift towards digital banking, increasing fraud pressures and creating new ones. Customers have been driven from the safety of store and branch visits to the vulnerability of the online marketplace. Added to this the pandemic has critically damaged the economy, resulting in cost pressures. This perfect storm has introduced many new and lasting dynamics: the traditional working week is unlikely to return soon; the onset of an economic recession and prolonged recovery; and the continued digitisation of consumer services will mean less physical competition on the high street. All of these factors increase consumers' exposure to fraud and economic vulnerability, leaving them more susceptible to fraudulent schemes.

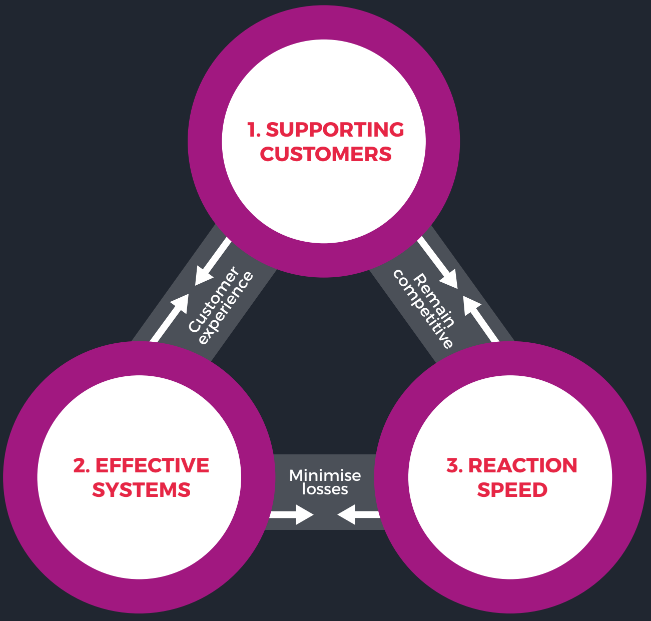
Trends suggest that banks are more likely to be at risk, although there are some clear actions they can take. We address the operational dynamics behind these challenges and outline how banks can prevent fraud losses, while better engaging and protecting their customers.

The critical pressures of fraud management

All banks will recognise the importance of delivering excellent customer experience to remain competitive and minimise losses.

We explore three critical pressures that can determine whether these imperatives are met successfully.

1. Supporting customers through engagement and education on fraud topics
2. Employing effective systems to detect, prevent and mitigate fraud
3. Operating with sufficient pace to keep up with the evolution of fraud attacks



1. Supporting customers: They are now more susceptible to fraud than ever

Remote working and more time spent at home gives criminal gangs greater opportunity to target consumers by calls, texts and emails. This increased availability, coupled with heightened economic vulnerability, has meant more customers are falling victim to fraudulent schemes. Social engineering or 'authorised push payment' (where customers are duped into transferring funds to fraudulent accounts) accounted for nearly £456m of losses in 2019, up from £354m in 2018. 2020 is on track to be at least the same, if not more – £207.8m (2020 H1) -v- £207.5m (2019 H1).[1]

The drive towards improving customer experience comes with its own risks of fraud. For example, over two million customers have signed up to open banking-enabled products since the introduction of the Payment Services Providers Directive 2 in 2018. While this has enabled innovative new products and services, it has also introduced opportunities for malicious applications that exploit them.

Social media is fertile ground for fraudsters. Young and ambitious social media users are recruited as 'transfer agents' for seemingly legitimate enterprises. They often unknowingly act as one of many within a chain of 'money mules', laundering stolen funds through their own personal accounts across multiple banks.

Fraudsters are continually evolving the way they take advantage of emerging social and technical susceptibilities. The lack of regulation around social media and technology companies has meant they cannot be relied upon in the fight against fraud.

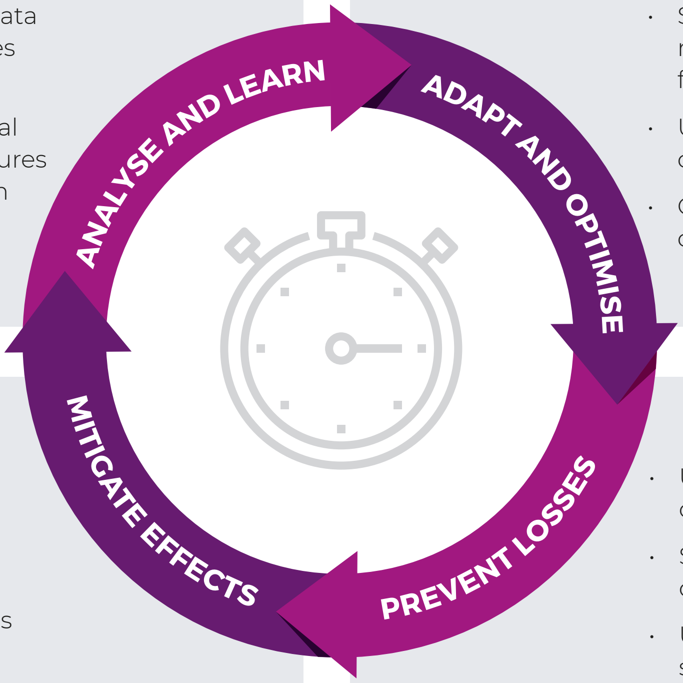
[1] 2020 Half Year Fraud Update | UK Finance

3. Reaction speed: Banks cannot react quickly enough

Banks are typically large and bureaucratic institutions. They have evolved broad and complex functional departments that require a high degree of independence to operate. Where there are overlaps between functions, the handoffs and governance between teams have been developed in an ad hoc manner and without holistic consideration. The unintended consequence of this organic evolution is misaligned authorities and responsibilities, creating destructive tension and uncertainty. The result: slow and divisive decision-making that cannot keep up with the evolution of fraud.

In addition to the slow decision-making, banks often lack investment in fraud capabilities and systems. Without this investment, they are unable to gather insight to predict future fraud schemes. Once fraud vulnerabilities are uncovered, banks face an uphill battle. They must either rely on crude controls to refer or block more transactions, or accept higher loss levels, both of which are sub-optimal outcomes.

Key reaction speed inhibitors



- Lack of advanced data analytics capabilities
- Misalignment between operational performance measures and customer harm measures

- Sluggish decision-making across functions
- Unreliable systems change execution
- Opaque insight into controls performance

- Excessive process handoffs between teams
- Ineffective self-resolution measures

- Unrealised potential for customer outreach
- Stagnant progression of prevention rule sets
- Unintegrated IT systems

> **Banks have had to continually implement controls to confront the ever-evolving threat of online fraud.**

Banks are best placed to help their customers avoid falling victim to fraud. However, many banks engage in generic mass marketing campaigns that lack creativity and inspiration when it comes to customer engagement on fraud. Most customers disassociate themselves from fraud believing it won't affect them. So sending them communications on the latest fraud schemes does not guarantee educational uptake. In many instances, it is this very lack of knowledge that exposes customers to fraudulent schemes, as reflected in the increasing number of social engineering tactics. In contrast to the impersonal fraud communications authored by banks, victims of fraud face an extremely personal and harrowing experience.

2. Effective systems: Legacy infrastructures and frameworks cannot cope with mass migration to online

High street branches are becoming increasingly under-utilised as consumers switch to more convenient and safer (during the pandemic) digital banking services. As this trend grows, it places greater importance on optimising the balance between a frictionless omnichannel customer experience and the right level of alerts and transaction blocks to minimise losses.

An increase in online transactions puts additional pressure on operational leads to deal with customer demand. Typical fraud prevention system false positive rates can be as high as 70:1[2], illustrating the demand on fraud operations to resolve these referrals and blocks. Costs must be controlled, therefore scaling the workforce with increases in online transaction volumes is not a sustainable response.

Banks have had to continually implement controls to confront the ever-evolving threat of online fraud. Banks could ease controls to reduce the volume of fraud investigations, subsequently providing a smoother customer experience – particularly for those who have yet to invest in customer self-resolution capabilities. However, risk functions do not have the systems and tools to provide them with adequate insight to sanction such trade-offs at the pace required.

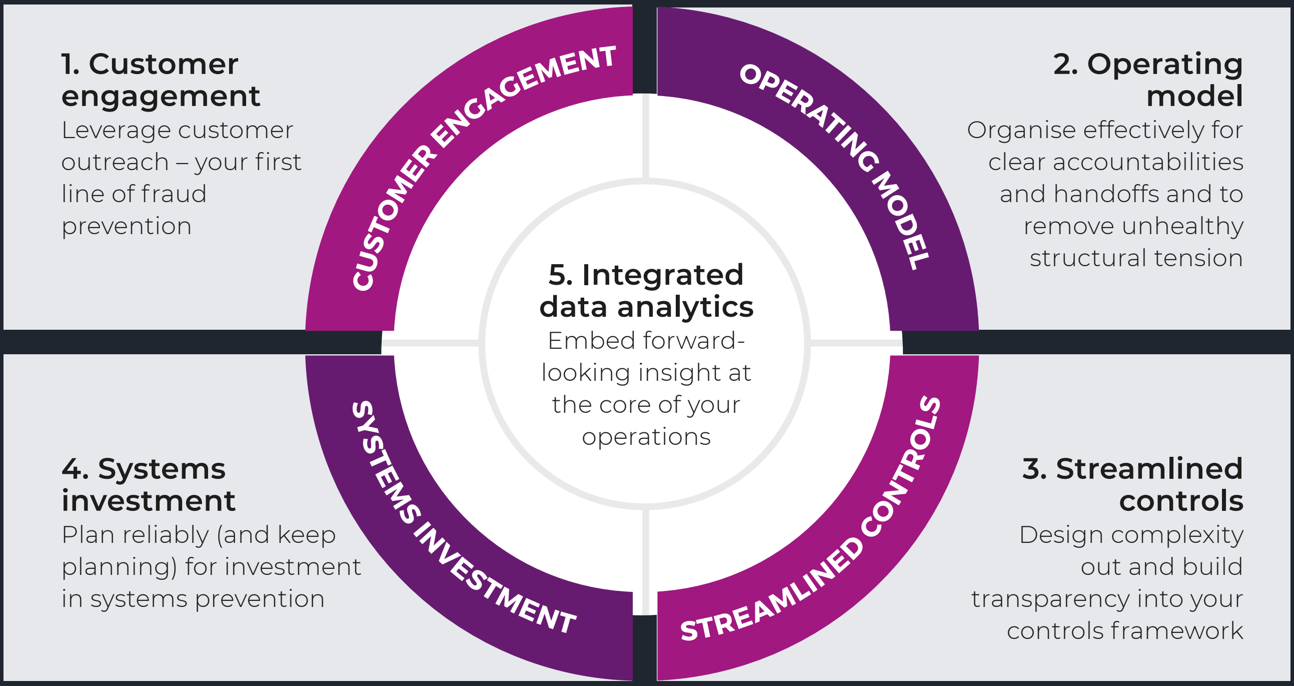
Control frameworks that are built up without a data-led, holistic approach can become increasingly complex. In such cases, unnecessary duplication and inconsistency of application and assurance are likely, all of which leads to a lack of awareness and confidence in the prescribed risk framework. It can also lead to undesirable behaviours, such as lack of compliance or even the development of local, 'off-grid' controls. Faced with increasing transaction volumes, misunderstanding and misapplication of controls prevails and creates further risk.

Banks that have not strategically managed their controls frameworks or consistently invested in upgrading fraud management systems will struggle to implement effective anti-fraud platforms and tools. Their fraud teams undertake low-value detection and mitigation activities, hindered by a constant and time-consuming battle to balance capacity and cost. They are inevitably being overwhelmed by the rising tide of online transactions.

[2] Gate One research

A practical solutions approach

Mitigating fraud loss is easier said than done. We have identified **five critical areas** where transformation will drive improvement.



1. Customer engagement
Leverage customer outreach – your first line of fraud prevention

2. Operating model
Organise effectively for clear accountabilities and handoffs and to remove unhealthy structural tension

5. Integrated data analytics
Embed forward-looking insight at the core of your operations

4. Systems investment
Plan reliably (and keep planning) for investment in systems prevention

3. Streamlined controls
Design complexity out and build transparency into your controls framework

1. Prioritise customer engagement

Banks need to utilise the rich information they have on their customers to provide customised or archetype-based information on the dangers of fraud relative to their respective financial behaviours. For example, customers who pay their bills through online banking should be warned of the dangers of relevant payment scams, while customers who use their bank cards abroad should be made aware of travel-related threats. At the very least, banks should identify the customers who have been exposed to fraud in the past and send them educational nudges, via their app or elsewhere, about how best to be cautious. This includes vulnerable customers who rely on others to fulfil their banking activity.

Ultimately, customer outreach and education is the first and best line of prevention and can potentially reap high returns on investment. Consider habit-forming behaviours, gamification and even random warnings to help customers learn and safeguard against fraud.

In addition, partnerships with credit agencies, for example, can allow banks to bolster their banking products with bundled benefits, such as security insights and recommendations. Even something as simple as employing a more empathetic language and terminology when referring to fraud victims can help banks build a more valued relationship with their customers to drive loyalty, reduce repeat victims and increase fraud intelligence.

Transparent and customer-focused controls

CLARITY FROM CUSTOMER EXPERIENCE TO RISKS, TO CONTROLS, TO STRATEGY

I MAKE AN APPLICATION

I decide I want to become a customer, so I submit an application online via the website

KEY RISKS

Applicants provide incorrect information to gain access to products and services and/or a better outcome

EXAMPLE CONTROLS

Fraudulent application protocols
Application fraud team and application detection systems monitor customer applications for potential fraud

Owner: Operations Controls Lead

CONTROL EXECUTION

Process	Owner
Data matching alerts	Fraud ops
Fraud check alerts	
Address check alerts	
Fraud scorecard alerts	
Video ID validation	Digital

QUALITY CHECKING

Measure	Data owner
£ losses mapped to application MOs	Insight and analytics
% penetration rate for alerts	
% compliance for alert processing	

Test owner: Control owner
Test frequency: Bi-weekly
Test support: Assurance team

QUALITY ASSURANCE

Example tests of appropriateness, adequacy and effectiveness

- Are the application detection rule sets optimised and updated effectively?
- Are staff trained comprehensively on how to process an alert?

Assessor: Control owner
QA frequency: Monthly

I ACCESS MY ACCOUNT

I register for online and telephone banking and start to track my spending on a regular basis

Customer details are compromised, allowing fraudsters to make transactions on their behalf

Telephone banking and digital credentials
Access to customer accounts are protected through a series of account management security protocols

Owner: Systems Controls Lead

Process	Owner
Digital registration confirmation email	Telephone and digital
Telephone banking password security	
One-time-password generation	

Measure	Data owner
£ losses relating to access breach MOs	Insight and analytics
% prevention rates	
Sign-in alert performance	

Test owner: Control owner
Test frequency: Weekly
Test support: Assurance team

Example tests of appropriateness, adequacy and effectiveness

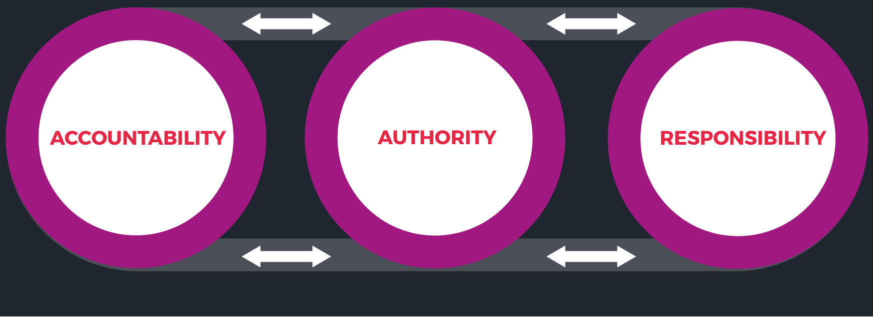
- Are our outbound confirmation emails safely constructed and sent?
- Are staff consistently applying telephone banking password requirements?

Assessor: Control owner
QA frequency: Monthly

STRATEGY

Outputs from assurance flow into strategic planning processes for risk and controls

Clarity of cross-functional decision-making is key



2. Organise effectively, as well as efficiently

While there is no single or best means to organise fraud risk and operational activity, fraud analytics should be at the core of your operations. These analytics should be intrinsically linked with fraud controls to continually drive pace in the fraud prevention and mitigation process. Where other teams sit, such as systems, change, investigations, customer operations, governance, etc, will depend on the organisational principles for each institution.

In the pursuit of operational efficiencies, many banks neglect process effectiveness, in particular process governance. They strive for handoffs that are conducted with ease and a seamless co-ordination of activity. However, the reality is that effective decision-making frameworks are not in place, rendering processes ineffective and sometimes even counterproductive.

Managing banking fraud presents three competing objectives: reducing fraud losses, minimising operational costs and delivering a smooth customer transaction journey. Banks must be clear on who owns the decision to trade-off between these three factors and how they will measure performance. This requires clear and robust governance that enables slick handoffs, negates internal tensions and minimises unstructured co-ordination measures. The payoff is a cross-functional fraud defence that is aligned and optimised.

3. Streamlined and customer-focused controls

To effectively manage performance controls, banks must have a robust quality assurance regime. This should be data-driven with a clear set of objectives and key results, which can be measured using empirical evidence. Banks can also use innovative methods such as adversarial 'Red team' testing (test-to-failure) to ensure they are stress-testing their own controls harder than fraudsters can, but within a safe environment.

Quick execution of these controls requires clear governance and ownership of the data to ensure it is reliable and accessible, avoiding any misinterpretation and disputes. Additionally, an integrated data infrastructure will enable automation of controls across functions, improving reaction speed to fraudulent activity. Speed and clarity are crucial for making effective decisions when balancing customer experience with controlling losses.

Developing the controls framework around the customer journey will allow for a smooth service across all areas within the bank. The clear line of sight between the bank's fraud management activities and the customer journey allows for faster decision-making, balancing the losses and customer experience. It also ensures controls are outcome rather than process-focused.

Fundamentally, banks which operate a best-practice approach will ensure the design of their risk and controls framework aligns with their customer journeys and effectively integrates data from across the organisation.

5. Integrate data analytics as the core of your fraud operations and try to keep up

All banks have data analytics capabilities embedded into their fraud prevention operations. However, it’s not just the capability that’s important, but having it embedded as part of a nimble operation.

Laggards use data analytics primarily to understand losses, constraining it to being reactive. Eventually these insights are integrated to calibrate fraud algorithms, however the design lacks the required pace.

Leaders ensure data analytics sit at the core of their fraud operations, enabling them to:

- accurately forecast the next fraud tactic
- inform the optimisation of controls
- forecast operational capacity with increased precision
- develop advanced behavioural profiling of customers
- drive efficiency through the automation of fraud triaging.

Leaders integrate cutting-edge technologies to keep up with the pace of data and insights, using artificial intelligence and machine learning to reduce the need for manual intervention.

Perhaps most crucially, those accountable for fraud risk and data analytics must ensure they work collaboratively alongside one another. Data-led solutions can be extremely effective, but to be implemented at scale they must be executed without obstruction or else risk investments fall short of delivering lasting value.

> **While there are a variety of fraud platforms available, adding the latest and greatest is not necessarily the right answer.**

4. Strategic and sustainable investment in systems

Inadequate systems can result in key operational issues, such as an insufficient detection capability. This can lead to a reliance on tactical, rules-based controls and a lack of customer self-resolution tools, exacerbating capacity challenges at times of high-alert volumes.

While there are a variety of fraud platforms available, adding the latest and greatest is not necessarily the right answer. For example, bolting new systems on to antiquated architecture normally results in a more expensive, sub-optimal outcome. Instead, banks should reliably invest in a strategic technology roadmap that does the following.

- ✓ Modularises technology architecture incrementally for a more malleable, reliable and long-term environment.
- ✓ Integrates a singular fraud platform across all products and channels to optimise fraud prevention. This both simplifies the architecture and provides a unified view of the customer across their transaction activities.
- ✓ Establishes consolidated and automated data feeds to enable reliable, analytics-based prevention and intervention.
- ✓ Consistent platform updates to maintain system efficacy and continually improve artificial intelligence and machine learning capabilities.
- ✓ Delivers the capability assurances required to plan improvements across interdependent areas such as data analytics, risk controls and operational process improvements.
- ✓ Provides greater digital services to intelligently process and confirm questionable transactions with customers.

Such roadmaps do not address systems limitations overnight. However, they do help careful investment planning in the face of financial constraints.

ALEX MCEVOY | Partner
alex.mcevoy@gateone.co.uk

Alex has a wealth of transformation experience within the financial services sector. He has worked with board members and executive teams across insurance, capital markets and banking. Alex enjoys working hand-in-hand with clients to find innovative and practical ways to solve complex transformation challenges.

ABOUT GATE ONE

Gate One is a leading digital and business transformation consultancy focused on designing and delivering meaningful change for some of the world’s most interesting, innovative and influential organisations.

And finally…

When it comes to fraud, many banks have been operating in silos. In fact, in our experience, 50% of fraud losses are never recovered as funds are laundered between banks. Of course, banks consider each other as competitors. Collaboration is not ingrained in the industry but fraudsters don't operate according to bank silos. They shift stolen funds across banks in seconds and the harm they create is industry-wide. Banks need to consider their losses at a more collective level.

Better collaboration and information sharing between banks will result in better-informed reactions to fraud. In this spirit, there is no reason to conceal observed trends on fraud alert types. As fraudsters change tactics, a co-ordinated effort using the combined capabilities of prevention tools across banks would be hugely effective in minimising losses for all banks. But it's not just the banks that would stand to gain. Customers would also benefit from consolidated insights into how best to avoid falling for social engineering scams, mule recruitment campaigns and phishing/vishing attacks.

There is more to be done once fraud activity has been recognised, especially for authorised payments. Banks currently send each other recovery forms, informing of funds sifting through mule accounts. By the time the forms are processed, it's almost assured that the fraudster will have moved the money elsewhere, leaving little to recover.

Interestingly, transactions across banks leave electronic traces and systems can follow them, but a quick co-ordination process is required.

Lastly, some banks will point to the regulator, asking them to play a larger role in this co-ordination. While this thinking may have some merit, the reality is that oversight bodies are not geared to deal with the pace and co-ordination required. Banks need to work with regulators to agree solutions, but not entrust them to do the work for them.

Final remarks

Our recommendations are not easy to achieve. In many cases, they require significant changes to the way fraud functions think and operate. On the other hand, the business case is clear. Those that do not acknowledge or invest will need to either accept higher fraud losses (assuming they continue to refund customer transactions) or implement more stringent risk controls that will hamper the customer experience.

For banks that take on all of our recommendations, their innovations will lead to first-mover advantage, where fraud prevention can become a competitive capability and customer offering. At the end of the day, we place our money with banks to keep our hard-earned funds safe.

REF: P 24.1