Commercial Banking Fraud Survey

An industry view

June 2025

Contents

Introduction

Fraud is at the top of agendas for banks, financial regulators and governments worldwide. But focus has largely been on fraud threats against retail consumers, with fraud impacting commercial banking and corporate customers receiving far less attention.

That's partly a consequence of fraud in commercial banking being less visible – less public data on commercial banking fraud is available. Businesses that become victims of fraud can be less willing to share information on how systems and controls were compromised. Where data is available, comparisons across institutions can be difficult due to differences in the products being offered, variations in market footprints, differences in risk appetite and varying definitions of fraud.

While hard to quantify, it's clear from our conversations across the industry that fraud represents a significant risk both for banks and their commercial customers. As well as direct financial losses, fraud erodes trust in business, increases costs of doing business and hinders growth. Effectively preventing and detecting fraud against business is critical for confidence and prosperity. High-profile business collapses following cases of alleged fraud have emphasised these broader impacts and the importance of effective risk detection processes in lender credit decisioning and of establishing mechanisms to detect fraud early warning indicators to enable swift action to de-risk and mitigate potential losses.

Our banking clients also tell us that they are seeing fraudsters increasingly target corporate customers in payment frauds, using the same social engineering techniques used to scam retail customers, enticed by the potential for larger pay-offs. Some businesses have publicly reported becoming victims of complex frauds that have involved cyber breaches and technologies like GenAI deepfakes, pointing to increasing sophistication of threats against business. The consensus across the industry is that payment fraud attacks and scams targeting businesses will only increase in frequency and sophistication.

Our analysis considers:

How banks are approaching fraud risk management and developing overall fraud strategy in a commercial banking context.

How banks are managing 1st party credit fraud risks when lending to medium and large businesses.

How banks are implementing measures to protect commercial customers from payment fraud risks.

It is in this context that we have performed this market survey to build a picture of how banks are developing anti-fraud capabilities to address changing fraud risks in commercial banking.

This report summarises our key findings based on information we have gathered through conversations with fraud teams at some of the world's largest international commercial banks. As well as drawing on insight from our work across the market, we have interviewed representatives from banks with large footprints in the US, the UK, Europe, Africa and Asia. Contributions by the banks involved are unattributed.

A key feature of all of our conversations with participant banks has been the desire to work together to defeat fraudsters and to strengthen prevention and detection at an industry-level. Our aim for this survey has been to explore how the industry is evolving its response and to call out features of leading practice to support industry-wide development of more effective anti-fraud strategies.

We would like to thank the institutions that have been part of our research for the time they have spent and their valued contributions to this analysis.

Headlines

01

How are banks approaching fraud risk management and developing fraud strategy in a commercial banking context?

- All the banks we spoke to had established specialist commercial banking fraud teams and mature anti-fraud capabilities. Ownership of fraud risk management consistently sat in the 1st line of defence.
- Three banks had specialist fraud teams in both the 1st and 2nd lines of defence, three had specialist fraud teams in the 1st line only and one had a specialist fraud team in the 2nd line only.
- All but one of the banks we spoke to had documented strategies to tackle fraud in their commercial banks.
- Definitions of fraud risk appetite and metrics used to monitor fraud levels varied across institutions.

02

How are banks managing 1st party credit fraud risks when lending to businesses?

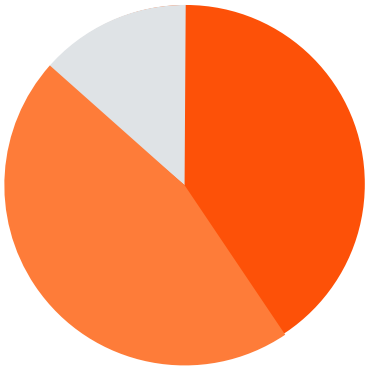
- A key distinguishing feature in approaches was variation in definitions of fraud and the evidential bar for loss events to be categorised as fraud.
- Some banks classified cases as fraud only where wrong-doing had been 'confirmed' – e.g. where there was sufficient evidence to support legal action against the borrower. Others classified cases as fraud where fraud was suspected on the 'balance of probabilities'.
- This variation led to significant differences in apparent numbers and values of loss events between banks of broadly comparable scale: some reporting 100+ fraud events with others less than five in the same period.
- Approaches to mitigating 1st party credit fraud were universally incorporated into KYC, credit origination and approval processes, with the key variation being the extent to which dedicated fraud teams had been established to investigate suspected fraud and the level of investment in fraud detection technology and analytical capabilities.
- Three banks had built technology solutions to proactively identify fraud early warning indicators in credit applications and in customer transaction activity.

03

How are banks implementing measures to protect commercial customers from 3rd party payment fraud risks?

- 3rd party payment fraud was identified as a significant and growing threat to commercial banking customers. All banks reported rising attack volumes, in particular impersonation frauds and business email compromise.
- Across the industry, investment has been channelled into payment authentication technologies and into payment screening tools to enable interventions in suspect payments.
- A key challenge in interventions was the high level of 'catch and release' where customers still proceeded with payments despite being warned that they might be fraudulent.
- There was significant variation in strategy around 3rd party payment fraud with the largest international banks having formally defined roadmaps to reduce customer liable fraud losses with performance metrics being monitored through governance forums. Other banks monitored customer liable fraud losses but did not have formal KPIs or a documented strategy to reduce customer losses.

Overall risk management approach



- Banks with fraud strategy subject to governance committee approval
- Banks with strategy document owned by fraud team but not subject to governance committee approval
- Banks with no formally documented commercial banking fraud strategy

All the banks we spoke to have mature anti-fraud capabilities within their commercial banking divisions, with anti-fraud measures embedded into customer onboarding/'KYC' and credit origination processes and a range of payment authentication and screening tools in place to detect suspicious customer activity and payments. All the banks we spoke to describe having a range of systems and controls in place to prevent and detect fraud, with programmes of planned enhancement activity to keep pace with changing fraud threats.

Overall approaches to fraud risk management shared many similar features across institutions but there was variation across three key themes which we explore in more detail in this section:

- Organisational structures and allocation of responsibilities across the lines of defence.
- Development and ownership of overall fraud strategy.
- Definitions of fraud risk appetite and fraud risk metrics.

Differences in the overall fraud risk management approach across these themes appear to have driven different cultures around fraud, and the level of investment in technology-driven approaches to prevent and detect fraud which we explore further in this report.

Organisational structures and the line of defense model

Ownership of fraud risk sat within the 1st line of defence at all of the banks we spoke to. All the participating banks had also established specialist fraud teams focused on threats impacting their commercial banking business. However, we observed different approaches to where these teams sat across the lines of defence with three key models across the surveyed banks.

Fraud teams located in both 1st and 2nd lines of defence

- 1st line team owns fraud strategy and is responsible for fraud risk management approach and operation of controls in collaboration with front office teams.
- 2nd line team sets control standards and oversees the design and effectiveness of controls. Specialist fraud team typically within either the Financial Crime or Operational Risk functions.

Fraud team in the 1st line only

- 1st line team owns fraud strategy and overall risk management approach with challenge and oversight provided by other functions such as Operational Risk and Credit Risk.

Fraud team in the 2nd line only

- 2nd line fraud team sets policy and standards with fraud controls operated on a decentralised basis by a range of other functions (business support teams, Operational Risk, Credit risk, etc.).

1st line fraud teams were either structured to align with business segments (for example, with fraud specialists focused on specific product areas or markets) or operated on a centralised basis for the commercial banking business as a whole with sub-teams organised by fraud risk type (most commonly with teams divided between 'payment fraud' and 'non-payment/lending fraud' teams) and then further divided with specialists focused on 'Strategy', 'Analytics', 'Technology' and 'Operations'.

1st line fraud teams were typically led by Managing Director-level individuals who acted as the fraud risk-type 'oversight officer'. One bank we spoke to had designated fraud oversight officers for each business segment as well as a central oversight officer looking across all business segments holistically. 1st line teams were typically responsible for:

- Fraud risk management governance.
- Fraud risk identification and assessment.
- Setting risk appetite and providing approval for residual risks.
- Operating anti-fraud systems and controls in accordance with defined standards.
- Generating and reporting fraud metrics and management information.
- Escalating and responding to fraud incidents.

The very large global banks we spoke to had centralised global fraud functions, and typically fraud teams and oversight officers were agnostic to geography. The larger banks we spoke to also had fraud subject matter specialists located in each region to support local business and address market-specific nuances. It was also common to see shared service centers operating fraud controls across markets and across business divisions. For example, investigations capabilities for credit/debit card alerts were often shared across retail and commercial banking divisions.

2nd line fraud teams typically operated on a global basis to set consistent standards across the bank's global footprint, and were commonly structured with specialists focused on 'non-payments/lending fraud' and 'payments fraud' (as well as internal fraud in several cases). The size of 1st and 2nd line fraud teams varied significantly based on the scale of the institution and its global footprint, with 1st line team's headcount being heavily skewed towards operations teams.

Approaches to organisational structure and allocation of responsibilities for fraud across the lines of defence had consequences for the overall approach. In particular, the bank that only had a 2nd line fraud team and operated controls on decentralised basis appeared to have less clearly defined business ownership for fraud risk and consequently a less clearly defined and cohesive fraud strategy.

Development and ownership of overall fraud strategy

Three of the banks we spoke to had formally documented commercial banking fraud strategies that defined short term objectives and long-term ambitions (5+ year time horizon) to strengthen fraud defences. Some of the banks we spoke to had defined fraud strategies covering all aspects of commercial banking as a whole, while others had separate strategies for each business area.

These strategies were developed as a collaboration between the 1st and 2nd line of defence teams, and were subject to formal review and approval by governance forums (typically those forums responsible for non-financial risk/Financial Crime) on a periodic basis. The creation of these strategies and their sponsorship by senior stakeholders appear to be a key element of driving change and building business cases around improvements to fraud systems, processes and controls.

Three other banks we spoke to had more informally defined commercial banking fraud strategies, described as being more focused on the roadmap of operational improvements such that they had less formal executive-level sponsorship. The bank with the decentralised risk management model had no formally defined commercial banking fraud strategy, reflecting the more diffuse ownership of fraud risk management across the range of different functions operating anti-fraud controls.

Risk assessment and appetite metrics

All the banks we spoke to had established processes to identify and assess fraud risks and had defined risk appetite metrics. Approaches to fraud risk assessments varied with some banks performing stand-alone annual fraud 'threat reviews' with granular analysis of trends in fraud attack types, by typology, product and payment channel. Others relied on higher-level annual enterprise-wide risk assessment processes to capture and refresh assessment of fraud risks. Fraud risk assessment was also cited by the banks we spoke to as a common element of new product approval processes, although the involvement of fraud specialists in these processes ranged from informal input to formal, policy-driven requirements for consultation and sign-off by fraud experts.

Fraud metrics typically covered a range of risk and control effectiveness factors including absolute measures of loss, numbers of fraud events and identified control issues. One of the banks we spoke to had established reporting thresholds to escalate on the basis of both 'warning levels' and 'breach levels'.

Fraud risk metrics were typically presented on a rolling 12-month basis, and distinguished between:

01 1st party credit fraud metrics

Absolute measure of loss by value

Percentage of total expected credit loss

Most banks monitored 1st party credit fraud both in terms of absolute losses and also as a percentage of total expected credit losses.

These metrics were typically co-owned and monitored by the Credit Risk function and an accountable executive for fraud.

02 3rd party payment fraud

Absolute measure of loss by value (split BY bank/ customer liable)

Net customer loss rate

Percentage of revenue

- 3rd party payment fraud was typically measured in terms of customer and bank liable fraud losses (net of recoveries).
- Some banks also monitored net losses per customer.
- Some banks were exploring how to measure payment fraud levels as a percentage of revenue to reflect fraud as a 'cost of doing business' which should be expected to grow in absolute terms as transaction volumes and values increased.

03 Internal fraud

Absolute measure of loss by value

Number of fraud events bucketed by value

Internal fraud was commonly measured on the basis of absolute loss with some banks reporting numbers of events, bucketed by ranges of value.

It was common across all the banks we spoke to have defined key operational indicators such as payment intervention rates, card decline rates, and 'catch and release' (i.e. cases where the bank intervenes in a payment which is subsequently released by the customer and later identified as being fraudulent).

In addition to these high-level fraud metrics, some banks had developed standardised fraud taxonomies that were applied across markets to consistently classify fraud events. This allowed the banks in question to monitor fraud losses (whether customer or bank liable) by underlying threat types and to track trends to inform forward looking enhancement activity. Payment fraud metrics were also often broken down by payment channel.

1st party credit fraud risk

Approaches to managing fraud risks in lending shared many consistent features across the banks we surveyed with fraud-related controls embedded into credit decision processes, in-life monitoring and the management of distressed debt. Reported numbers of loss incidents and loss values varied significantly between institutions driven by variation in risk appetite at origination, the nature of lending products offered by each bank, the overall size of the lending book and (as described further below) each bank's approach to classifying credit losses as fraud.

While the numbers and values of loss events varied significantly, banks highlighted similar types of fraud incidents with the most common being manipulation of apparent financial performance by borrowers.

The banks we spoke to described challenges of identifying what could be quite subtle indicators of manipulation in reported financial information with technology capabilities to identify anomalies in reporting being a key area of investment as described further below. Banks that offered trade credit facilities reported that the most common fraud schemes involved facility abuse, including through 'fresh air' invoicing, round tripping and credit note manipulation.

While the banks we spoke to generally felt that 1st party credit fraud risks had been higher in recent years as a consequence of rising pressure on businesses caused by global macroeconomic factors, those we spoke to were confident that systems and controls were effective at mitigating the most serious fraud cases with numbers of higher value loss events being very low. Appetite for investment was driven by the desire to improve capabilities to detect more subtle indicators of fraud at an earlier stage, enabling quicker action to address improper behaviours by a borrower and to de-risk the position.

Differences in approach to fraud definition

How banks define fraud varied significantly between institutions and was a key factor driving variation in apparent numbers of fraud cases. Survey participants of roughly comparable size reported very different numbers of fraud cases: one reporting 100+ fraud incidents with others reporting less than five in the same period.

Two broad approaches to classifying a credit loss event as fraud were applied:

Balance of probabilities

Credit loss events classified as fraud or suspected fraud where it was considered more than likely that dishonesty or deception were involved. Such dishonesty and deception need not relate to the specific cause of the loss event, but may relate to how the facility was initially acquired, for example, by providing false or misleading information at application.

Confirmed cases

Credit losses were only reported as fraud where there was strong evidence that fraud had occurred. Some banks indicated that they would only classify a case as fraud where there was sufficient evidence to take legal action against the borrower.

As would be expected, banks taking a 'balance of probabilities' approach reported much higher numbers of fraud cases than those taking a 'confirmed case' approach. A theme of our discussions with several banks was the benefit of classifying a loss event as fraud with some taking the view that calling something fraud after the loss event had occurred has limited benefit as it doesn't alter the way the case is managed or how value is recovered. However, others argued that classifying a case as fraud earlier had a number of important benefits, including:

- Providing an earlier trigger to de-risk the position on an expedited basis, even if no fraud were subsequently proven.
- Provoking a more robust investigative process to understand lessons learned and as a means to identify improvements to risk management approaches.
- Raising visibility of fraud risks and a more proactive culture around fraud risk management.

The banks we spoke to that had adopted a 'balance of probabilities' approach typically had invested more in systems and capabilities to detect fraud early warning signals and had more proactive approach to de-risk positions showing red flags. Senior management visibility and awareness of fraud risk was clearly a factor in building business cases to support investment which was driven by the high level of scrutiny of potential fraud cases the 'balance of probabilities' approach encouraged.

Risk appetite

All the banks we spoke to had defined 1st party lending fraud risk appetite thresholds, with one of two approaches typically being applied. Banks either measured fraud losses in absolute loss terms, setting a risk appetite as a total loss value or as a percentage of the expected credit loss provision. The level of appetite, however defined, was impacted by the bank's approach to the definition of fraud.

There was recognition that fraud loss rates could be significantly impacted by one-off larger events, and generally the banks we spoke to describe the risk appetite number as being a 'moving target', often driven based on loss rates in the prior year. Those we spoke to described risk appetite primarily as a means to drive a conversation about fraud risk across the business and whether improvements to processes and controls were required.

Origination

Fraud systems, processes and controls

Fraud systems, processes and controls were generally described as being applied in three stages: at origination, in-life and post-distress event. While control approaches shared many similar features across banks, a key difference was the extent to which technology solutions had been developed to automate or enhance manual review processes. Where banks had adopted technology enabled approaches, a common challenge was that different systems operated as point solutions with limited ability to join the dots across different platforms to provide a more holistic picture of risk.

- All banks had embedded anti-fraud processes and controls in the credit approval process with a common approach being to require relationship managers/deal teams to address questions explicitly considering fraud risk at origination.
- It was common for fraud risk assessments to be reviewed and challenged by specialist fraud teams where these existed in the 1st line of defence. For larger exposures, fraud specialists were often embedded in deal teams providing ongoing support and analysis as part of the overall risk management approach.
- A key difference across the banks we spoke to was the extent to which technology was deployed at this stage. Some banks relied on manual analysis of information (such as financial statements) to identify anomalies and fraud risk indicators. Some banks had built technology capabilities that analysed financial information to automate the identification of risk signals.
- Where technology was used, systems were typically in-house built and the more sophisticated systems drew on a wide range of bank and external data to evaluate the customer's apparent performance against peers in their specific market sector as well as applying more standard rules-based anomaly detection approaches.
- The extent of reliance placed on borrower financial information being subject to audit varied across institutions, with the identity of the auditor (e.g. large/small firm) being cited as a factor considered by some banks we spoke to.
- Where banks offered asset finance facilities, independent valuations experts were common across the banks we spoke to, in particular for specialist or higher value assets.

In-life

- Periodic reviews of credit facilities and regular review of customer MI and forecasts were a consistent part of the risk management approach across all the banks we spoke to. Some banks described these processes as involving specific requirements to refresh fraud risk assessments.
- As with the origination stage, the key distinction across banks was the extent to which technology and automation was being applied to identify fraud risk indicators for in-life facilities. Some larger banks had invested in technology solutions to provide sophisticated monitoring and detection capabilities, in particular in relation to trade credit facilities. Banks investing in these capabilities typically described their objective as being to identify fraud warning signals earlier, enabling accelerated action to de-risk the position.
- Some banks had also built their own analytics tools to operate in parallel with credit platforms and risk management systems to identify anomalies and signs of manipulation. One bank noted that they were adopting AI to perform analysis of financial statements and other information, including to detect forged and manipulated documents.
- Where risk indicators were identified, it was common for banks to have dedicated lending fraud investigation teams who worked alongside distressed loan teams. These teams were described as being staffed by fraud experts with experience in the analysis of financial information and corporate intelligence research in the context of fraud.
- These teams advised distressed loan teams in relation to indicators of fraud, and where fraud was suspected, they work alongside Financial Crime and Legal teams to report suspicions externally and to recover value where possible.

Recoveries

- Fraud teams at the banks we spoke to were keen to pursue losses both to recover value where possible and also to deter future wrong-doing, but often described encountering resistance within their hierarchies.
- This was primarily due to a concern about throwing 'good money after bad' that made it hard to justify the use of the asset recovery or specialist distressed asset teams.
- There was a general view that more coordinated action is needed to prevent bad actors taking advantage of multiple institutions and to deter wrong-doing generally. Banks we spoke argued that this would require involvement from government and law enforcement to encourage more proactive approaches.

Payment fraud risk

3rd party payment frauds targeting commercial banking customers were consistently called out as a rising threat, with impersonation frauds and business email compromise being the two most common attack types. One bank we spoke to indicated that they had experienced a five-fold increase in attacks targeting their customers in the last two years, with commensurate impact to alert and investigation case load.

Survey participants noted that increasing international regulation around consumer fraud protections (e.g. the UK Payment Systems Regulator's mandatory reimbursement regime) had concentrated attention on fraud prevention and detection into personal banking. While this level of focus was positive and had led to development of new payment screening technologies, some banks commented that it had detracted from focus on commercial banking risks where there was no reimbursement obligation.

A key driver for investment across the industry was improving detection precision rates to minimise customer losses while also minimising false positives that required large operational teams to handle. 1st party payment fraud, for example BACS limit abuse, was also flagged as a risk by some of the participant banks, although this was much less common. Cheque fraud was cited as a significant headache for banks with large footprints in the United States, where cheque fraud investigations consumed a significant portion of operational capacity.

The banks we spoke to were closely monitoring threat patterns and several had established dedicated threat intelligence and horizon scanning teams to monitor criminal behaviour and to inform forward looking strategies and detection approaches.

Horizon scanning

All the banks we spoke to performed some level of fraud risk horizon scanning, although this varied in formality across institutions. Banks adopted a range of approaches including having dedicated individuals or teams responsible for monitoring threats and changing attack vectors, often with leadership by the Chief Security Officer and delivered through cyber-security teams.

These teams used a range of techniques and vendor tools, including monitoring criminal forums on the dark web, to generate insight into possible threats and to identify compromised customer payment credentials and login information. Bank fraud teams also regularly attended industry events and briefings to stay informed of recent trends, including workshops arranged by organisations like UK Finance, the Payments Association and the Association of Corporate Investigators.

Threats shared common patterns with those experienced across retail banking, with social engineering and cyber crime techniques being increasingly common as a means to either manipulate commercial customers' employees to transfer money to fraudsters or to compromise customers' systems to access sensitive information. All the banks we spoke to operated education programmes to inform customers about potential threats and to support customers to implement effective processes to mitigate risk. Customer education ranged from regular written communications and alerts sent via email, online security centres with a range of education material available for customers to read and online seminars and briefings for customers on the latest fraud trends. Some banks ran periodic bespoke education sessions for clients to focus on specific threats impacting their businesses.

Catch and release

Several of the banks we spoke to referenced the challenge of 'catch and release' – cases where payments had been flagged as suspect fraud by the bank but which were confirmed by the customer and released but subsequently reported as fraud. One bank referenced that they had launched an extensive education campaigns (both for bank operational staff responsible for delivering warning alerts to customers and to the customer's staff themselves on how to effectively validate payment details) to bring catch and release rates down from 7/10 to 2/10 payments being reported as fraud having previously been flagged to the customer but subsequently released.

A key challenge in managing catch and release was ensuring customers had robust processes to verify payment information, for example, when performing call backs to verify changes to supplier payment details. Key lessons for business customers focused on.

01

Importance of independently sourcing contact information to perform call backs rather than relying on contact information on documents apparently received from a supplier.

02

Training staff with access to payment information on the dangers posed by business email compromise and the importance of applying professional scepticism when receiving instructions from counterparties to change payment information or to make payments.

03

Being alert to social engineering techniques where payments were requested urgently or where payment instructions appeared out of the ordinary.

04

Highlighting the risk of criminal use of deepfakes and voice clones and challenging unusual payment related instructions, even where these might appear to be from trusted members of staff.

Prevent and detection

Approaches to preventing and detecting payments fraud were broadly consistent across the banks we spoke to. The majority of banks we interviewed leveraged card fraud detection and investigation capabilities that were shared with their retail banks. All the banks had implemented a range of authentication methods for digital payments including multi-factor authentication and biometrics for login and payment instructions, dual authoriser requirements for large payments and device profiling to detect unusual login activity.

The configuration and application of these control elements varied across institutions, and by payment platform (for example, whether customers accessed payment systems through a bank-provided portal or through back office system integrations) and based on customer specific requirements and preferences. Several of the banks we spoke to had also built capabilities into payment systems to generate warnings where potential risk factors were identified.

All of the banks we spoke to had implemented payment screening systems to flag and pause suspect payments which required customers to confirm the payment information before it was released. These systems were evenly split between in-house developed capabilities and vendor solutions.

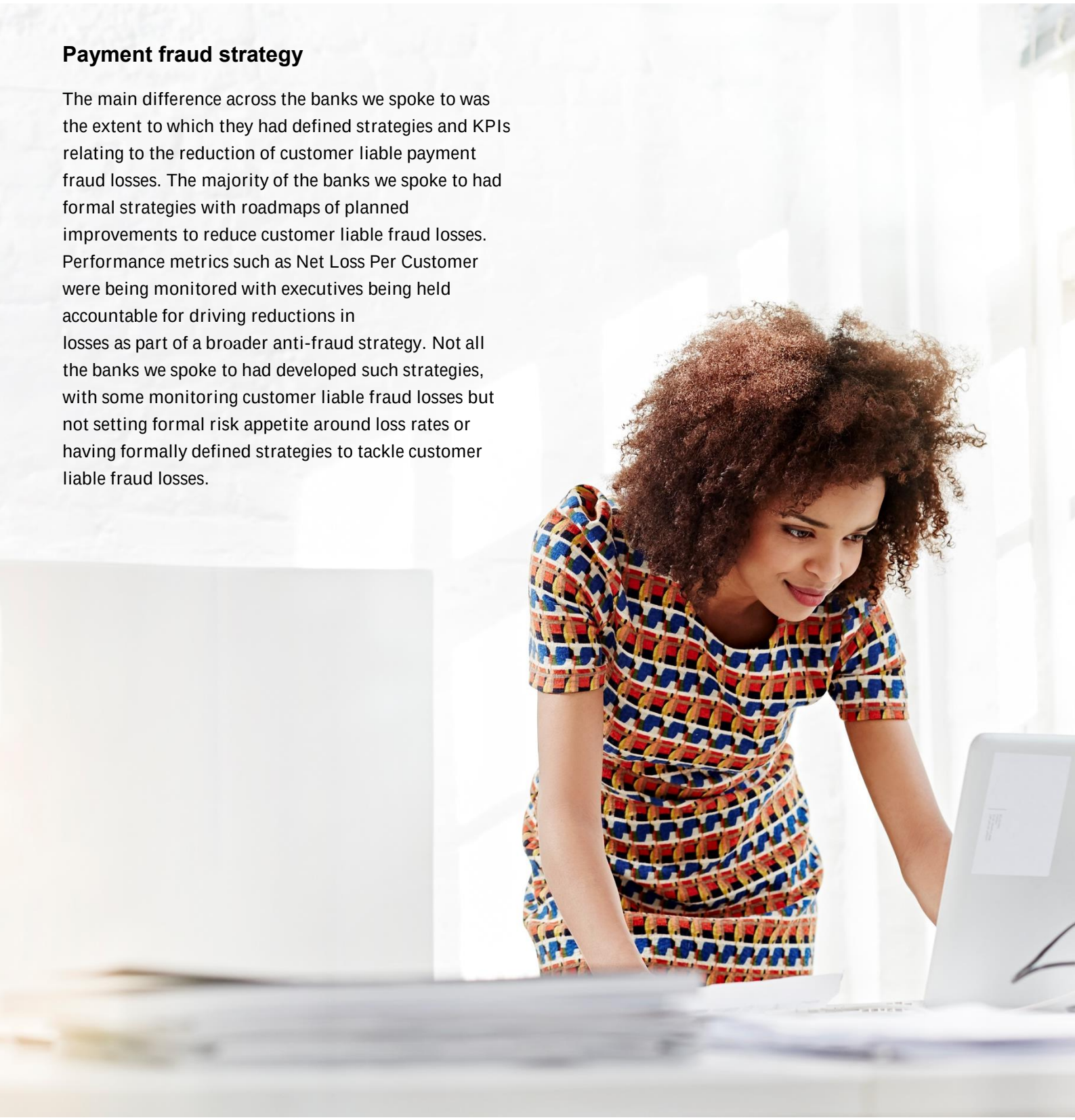
While rules-based approaches were common, many of the banks we spoke to were transitioning to model-first approaches to improve detection accuracy and flexibility to tackle changing methods of attack. One bank we spoke to indicated that their detection system operated on an 80:20 models versus rules basis, with another bank at the other end of the spectrum indicating that their approach was 20:80 models versus rules.

Generally the banks we spoke to indicated that improvements in detection capabilities had led to overall reductions in client loss rates over the last 2-3 years, despite significant increases in attack volumes. One bank indicated that investment in new model-based detection capabilities had led to customer loss rates reducing by 50% in recent years.

Commercial customers consumed payment fraud alerts in a number of different ways with more sophisticated customers receiving alerts through a digital journey integrated with their back office finance systems. However, banks told us that the majority of fraud alerts were resolved by direct outreach to the customer by Operational teams, typically by telephone, leading to high operational burdens to manage alert volumes.

Payment fraud strategy

The main difference across the banks we spoke to was the extent to which they had defined strategies and KPIs relating to the reduction of customer liable payment fraud losses. The majority of the banks we spoke to had formal strategies with roadmaps of planned improvements to reduce customer liable fraud losses. Performance metrics such as Net Loss Per Customer were being monitored with executives being held accountable for driving reductions in losses as part of a broader anti-fraud strategy. Not all the banks we spoke to had developed such strategies, with some monitoring customer liable fraud losses but not setting formal risk appetite around loss rates or having formally defined strategies to tackle customer liable fraud losses.



Conclusions

While it is hard to compare fraud loss rates or the 'success' of different organisation in managing fraud, we observed a clear spectrum of approaches with leading practice being differentiated by:

All the banks we spoke to had mature anti-fraud capabilities across both 1st party credit fraud and 3rd party payments fraud, but there were significant variations in approaches across the banks we interviewed. We observed a range of operating models, differences in the ownership of fraud from an overall risk management perspective and variation in approaches to strategy, risk appetite and the definition of fraud.

Ownership and accountability for fraud risk being clearly defined within the business.

Levels of investment in new technologies to improve the effectiveness and efficiency of fraud detection systems.

Robust monitoring of fraud and high organisational awareness of fraud risks, including losses borne by customers as well as those impacting the bank.

Development of forward-looking fraud strategies that identified new and emerging risks and set longer-term objectives and ambitions for systems and control enhancement.

Banks where we observed these leading practices were beginning to focus on how to bring a more cohesive approach to fraud risk management across the bank. As one bank put it, 'sweating the assets' being used across the bank but in different operational silos or risk areas was key to maximising value. With threat volumes rising and risks becoming more complex this kind of operational integration was seen as key to driving efficiency and effectiveness of fraud capabilities.

All the banks we spoke to recognised that fraud was a constantly evolving risk and that controls needed constant adaptation to address changing threats. Across the survey, we observed that the banks that had the right foundations – an effective organisational model and clear risk ownership in the business – had been better able to define and deliver business cases for broader improvement of fraud systems and controls.

How PwC can help

We support global organisations across a wide range of sectors to understand and manage their exposure to fraud risk. Within our team we have specialists focused on fraud risk in a banking and payments context that work extensively with international financial institutions to help them protect their businesses and their customers from fraud.

We have worked with some of the world's largest financial institutions to improve their response to fraud, delivering sustained and measurable improvements to fraud risk management approaches. For further information, reach out to the contacts on the following page.

Understanding risk

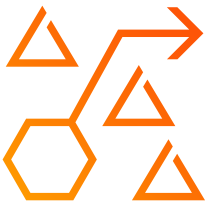
We support banks to understand fraud risk exposures across different markets, product lines and channels, including providing threat intelligence based on the latest fraud trends and criminal chatter.

Assessing capabilities

We perform independent assessments of people, process and technical capabilities to identify ways to enhance anti-fraud capabilities in light of our view of leading industry practices and considering proportionality to risk.

Developing fraud strategy

We support clients to develop forward looking strategies to deliver future-ready fraud risk management. We help clients develop business cases for investment in new capabilities to drive reductions in fraud losses, improve operational efficiency and to deliver better customer experience.



Driving fraud transformation

We support clients execute transformation plans by assisting with the design, selection and implementation of anti-fraud technologies and by driving efficient fraud operations through process re-design, automation and improved productivity.

Contacts

Harry Holdstock

Fraud and Regulatory Protection Leader
harry.g.holdstock@pwc.com
+44 7706 284348

Alex West

Banking and payments fraud leader
alex.e.west@pwc.com
+44 7841 567 371

Tom Roberts

Manager
thomas.x.Roberts@pwc.com
+44 7483 400 234

Genevieve Gimbert

Partner– Financial Services Advisory – United States
genevieve.d.gimbert@pwc.com
347-607-9465

Penny Dunn

PwC Risk Advisory | Partner – Australia
penny.dunn@au.pwc.com
+61 407 367 561

Jeny Rasheva

CEE Fraud Services Lead
jeny.r.rasheva@pwc.com
+359(0) 890 415 910

RITM0191613