BeyondFS

Fraud Strategy:

Building a Successful Framework for Your Organisation

Fraud is a constant, evolving threat to financial institutions, undermining stability, customer trust, and compliance. As fraudsters grow more sophisticated, the demand for adaptable, effective strategies has never been more urgent.

This guide explains how to develop an effective fraud strategy for your organisation, drawing on the extensive experience of BeyondFS. We have not only crafted such strategies but we have also implemented them—giving us a clear understanding of the key considerations and potential pitfalls to ensure success.

With advancing technologies, rising customer expectations, and tighter regulations reshaping the landscape, we offer a practical, real-world approach to building a strategy – to help you identify, prevent, track, and respond to fraudulent activity.

The Changing Fraud Landscape

The battle against fraud has become a high-stakes arms race, with financial institutions, regulators, and law enforcement working to stay ahead of increasingly sophisticated criminals. Fraudsters continually refine their methods, leveraging dark web tools and advanced technologies like artificial intelligence to exploit vulnerabilities. Unlike financial institutions, fraudsters face no regulatory constraints or oversight, allowing them to adapt quickly and operate with agility.

Meanwhile, financial institutions face mounting challenges:

- **Regulatory bodies,** responding to rising fraud levels, are imposing stricter requirements and demanding more proactive prevention measures.
- **Customers** expect seamless, secure services as standard, creating pressure to balance convenience with protection.
- Reflecting rising demand, the **tech vendor market** is overcrowded, with an overwhelming number of fraud prevention tools making it difficult to choose the right solutions.

To succeed, financial institutions must carefully balance security, compliance, and customer trust, while staying agile in the face of emerging threats. Collaboration with regulators and law enforcement is critical to prevent fraudsters gaining the upper hand.

Evolving Fraud Threats: External and Internal Risks

External Fraud	Internal Fraud
Synthetic identity fraud: Fraudsters combining real and fake information to create new identities, which are then used to open accounts and secure credit.	**Insider-assisted account takeover:** Employees colluding with external fraudsters to exploit privileged access and bypass security controls.
Deepfake scams: Using AI-generated video or audio to impersonate executives or customers to authorise transactions.	**Data poisoning:** Manipulating data fed into fraud detection systems to create blind spots or allow fraudulent activity to slip through.
API exploitation: Targeting vulnerabilities in open banking APIs to siphon funds or access sensitive data.	**Overpayment scams:** Collaborating with customers to initiate inflated refunds or overpayments, then siphoning off the difference.
Man-in-the-middle attacks: Intercepting real-time banking transactions or communications to alter payment details.	**Credential sharing:** Employees deliberately sharing system logins to obscure individual accountability in fraudulent activities.
Mobile app spoofing: Creating counterfeit versions of banking apps to steal credentials or facilitate unauthorised transactions.	**Session hijacking:** Exploiting unattended or insecure employee devices to perform unauthorised activities under their credentials.
Cryptocurrency-related fraud: Fake exchanges or wallets targeting customers or the bank itself in the digital asset space.	**Collusive loan write-offs:** Approving loans for accomplices and writing them off as uncollectible without due process.
Social engineering on steroids: Leveraging detailed personal data from data breaches or social media to manipulate customers or staff into revealing sensitive information.	**Behavioural data exploitation:** Selling customer activity data, such as spending habits, to external parties for profit.

Why Your Organisation Needs a Fraud Strategy

Without a clear, robust strategy, financial institutions are left exposed to significant risks, regulatory pressure, and reputational damage:

- **Fraud is evolving fast:** Fraudsters are evolving faster than organisations can react, leaving institutions vulnerable to significant losses. Emerging technologies like AI and the dark web help criminals outpace traditional defences, making adaptability essential.
- **Regulatory pressure:** Regulators are tightening fraud prevention requirements, with non-compliance risking fines and reputational damage.
- **Customer expectations:** Customers expect secure, seamless services; breaches erode trust, increase churn, and harm acquisition.
- **Resource limitations:** Limited resources mean you can't tackle every fraud risk at once—a strategy that prioritises significant threats will deliver better results.
- **Financial impact:** Fraud losses disrupt operations, drain resources, and hit the bottom line; a strategy can turn fraud into a manageable cost driver.
- **Technology investment needs direction:** Technology alone won't solve fraud; without a strategy, you risk investing in tools that don't address your unique challenges.
- **Cross-departmental challenges:** Fraud affects multiple departments, and without a unified approach led by a strategy they will operate as silos, leading to inefficiencies and gaps in protection.

Why Act Now?

Fraud isn't just an operational challenge—it's an opportunity for you to show leadership in a vital area. How effectively you address it can shape both your professional reputation and your organisation's resilience. Left unchecked, it becomes more costly, more disruptive, and harder to control, putting you on the back foot in a high-stakes race. That's why acting now is essential:

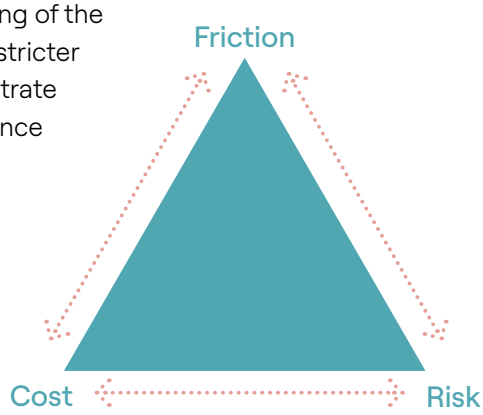
- **Take the lead in your organisation's future direction:** Map out where your fraud controls need to be—not just for the next six months, but for the next 2-3 years. This foresight ensures you'll be seen as having created a clear, cost-effective path to success.
- **Secure the resources you need for the long haul:** Multi-year planning, including future spending, ensures you can make the case for consistent investment and avoid last-minute scrambles for budget.
- **Keep fraud firmly on the leadership agenda:** An actionable strategy that highlights measurable improvements makes it hard for senior leadership to deprioritise fraud, keeping it central to your organisation's goals.
- **Enhance your standing as a strategic leader:** Drive a long-term fraud strategy that delivers tangible results, positioning yourself as someone who shaped a proactive, effective approach rather than reacting to crises.

Waiting means exposing your institution to escalating risks. Building a fraud strategy will drive a sustainable, forward-looking agenda and enhance your reputation.

How to Build an Effective Fraud Strategy

An effective fraud strategy provides a structured framework for informed decision-making, centred on the competing forces of reducing fraud, improving customer experience, and controlling costs. These goals form the corners of a triangle—prioritising one inevitably means compromising on the others to some degree.

A strong strategy requires a clear understanding of the trade-offs between these goals. For instance, stricter controls may bolster fraud prevention but frustrate customers, while prioritising customer experience could expose the business to greater risks.



Determining the ideal balance between these goals is key. Your priority goals, agreed with stakeholders, should underpin every action, from day-to-day operations to strategic investments, ensuring alignment with your organisation's wider goals.

The Strategy Development Roadmap

Creating a robust fraud strategy requires thoughtful planning, strong stakeholder alignment, and a focus on data-driven decisions. Here's a step-by-step guide to help you approach it with confidence:

1 Start with the big picture

Fraud doesn't exist in a vacuum—it's influenced by broader business and financial crime strategies. Begin by understanding the wider strategic context and constraints. Aligning with overarching organisational goals can strengthen your case for investment in fraud controls. Viewing fraud as a controllable cost driver opens opportunities to link fraud initiatives with improvements in customer experience, revenue, and operational efficiency.

2 Identify key strategic goals

Your fraud strategy must balance three competing priorities: friction, cost, and risk. While it's tempting to address all three simultaneously, it's more effective to identify and agree on clear priorities to guide initiatives and investments. Consider:

- What level of customer friction is acceptable?
- How does fraud impact customer acquisition or retention?
- What are the regulatory and financial risks of current fraud levels?

3 Assess the current state

A clear understanding of your starting point is crucial. This includes gathering meaningful data to understand what's happening today, why it's happening, and whether it's acceptable. If gaps exist in Management Information (MI) and reporting, prioritise fixing them as a first step.

Effective assessment involves:

- **Asking critical questions:** Focus on friction, risk, and cost. For example, can reducing friction improve customer experience? How do fraud rates compare to peers?
- **Being data-led:** Invest in trusted data capabilities, whether through internal teams or external expertise.
- **Avoiding analysis paralysis:** Fraud evolves quickly; concentrate on addressing the most significant risks first.

4 Prepare for action

With a clear understanding of the landscape and defined goals, shift your focus to execution. Effective implementation requires:

- **Engaging Stakeholders:** Fraud intersects with Compliance, IT, Customer Experience, and business teams in a way that other financial crime disciplines usually don't. Early collaboration and clear communication about the benefits of fraud initiatives can turn potential obstacles into allies.
- **Defining and Prioritising Initiatives:** A three-year horizon allows for phased improvements, including major changes like system upgrades. Prioritise initiatives based on impact and feasibility, but remain flexible as new challenges emerge.
- **Leverage Organisational Processes:** Align strategy implementation with budget and approval cycles. Solid business cases supported by trusted metrics improve the likelihood of securing funding and sustaining momentum.

5 Keep the strategy adaptive

Fraud threats evolve rapidly, so flexibility must be a core principle. Build mechanisms to monitor changes in fraud patterns, update defences, and adapt your strategy accordingly. Regularly reassess priorities, refine data insights, and maintain alignment with broader organisational goals.

FRAUD STRATEGY IN ACTION:

A Real Example from BeyondFS

The Challenge

- Our client, a major European banking group, had faced a surge in fraud levels, with over 30,000 fraud cases a year. APP Fraud incidents alone were 24% up, with gross losses of over £11 million.
- Multiple areas of the bank needed to engage in fraud prevention, including Financial Crime, IT, Operations and commercial functions. The bank lacked a cohesive fraud strategy, relying on disparate approaches and technology vendors, leading to inefficiencies, rising costs and regulatory concerns.
- Our client recognised the need for a globally applicable fraud strategy, aligned with their wider global strategy for digitisation and automation to support growth.

The Solution

- BeyondFS were briefed to prepare a comprehensive 3-year strategic plan for combatting fraud across the entire bank.
- Our small team of consultants had deep fraud prevention experience, enabling us to draw on lessons learned in other financial institutions. We identified the biggest and fastest growing areas of loss, and their causes. We also reviewed relevant regulatory requirements and identified areas where the bank was at risk of breach.
- We considered fraud across 5 key business areas (payments, cards, lending, internal, and investment fraud) liaising closely with the heads of fraud in each of these areas to align our recommendations with business needs.
- BeyondFS assessed existing technology infrastructure and vendors, recommending an approach for implementing new technologies and data analytics to improve fraud detection. A broader partnership with an existing vendor was recommended across payments, cards and lending, with a rollout strategy developed by BeyondFS.
- The fraud strategy prioritised customer experience, with easy-to-navigate channels for raising fraud concerns, obtaining information, and resolving cases. A fraud 'value proposition' was developed to help customers understand why procedures sometimes appeared more onerous than necessary, stressing the positive value of increased authentication measures.
- We created a model for collaboration across the bank's departments which aligned with the overall strategy. We also recommended an approach to knowledge sharing and cooperation with regulators to combat fraud across the wider industry.

The Outcome

- The strategic plan provided a clearly prioritised roadmap for the next three years. This was agreed by the board, with budget funding successfully secured for implementation.
- Cost savings and efficiencies were identified through vendor consolidation and data-driven analytics.
- Employee awareness of fraud was enhanced via an internal training strategy to improve understanding of fraud risk across the bank.

Client Outcomes at a Glance:

- 3-year roadmap to improve fraud prevention with budget and resource allocation secured.
- 5 key areas of fraud addressed across 6 countries.
- Efficiencies improved in the handling of 30,000+ fraud cases annually, through consolidation of technology vendors and process standardisation.

Key Considerations for an Effective Fraud Strategy

Fraud Technology

A well-defined fraud strategy is essential for selecting and implementing tools effectively. Flexibility is crucial—systems with no-code or low-code capabilities enable teams to adapt quickly to new threats without relying heavily on IT.

While fraud technology can be transformative, it is often oversold. Vendors may exaggerate capabilities, presenting their solutions as universal answers to fraud challenges. In reality, many tools address only specific fraud types, leaving institutions exposed to other risks. Systems that cannot adapt to emerging threats quickly become outdated, and lack of compatibility can hinder smooth integration into existing systems.

To make effective decisions, institutions should:

- **Begin with a thorough assessment:** Understand your fraud landscape, risks, and operational requirements.
- **Challenge vendors:** Have vendors demonstrate how their solutions address your specific needs.
- **Conduct proof-of-concept trials:** Validate vendors' claims in real-world scenarios.
- **Select adaptable, future-proof tools:** Choose technology that integrates well, demonstrates flexibility, and can evolve to address future challenges, for example using AI, biometrics, or advanced analytics.

Fraud Governance

Fraud not only evolves rapidly in terms of techniques, but it can strike with alarming speed. One day your organisation might seem secure, and the next, fraud can spiral out of control, impacting customers and operations instantly. This urgency demands frequent, dynamic risk assessments—annual reviews won't cut it. Leveraging shared industry data on emerging typologies ensures your organisation stays ahead of new threats.

Fraud's position between financial crime and operational risk calls for an agile, business-aligned approach. Clear accountability, budget control, and senior leadership involvement are critical to driving effective strategies and adapting to changes like new technologies or operating models.

With decisions spanning multiple departments, a collaborative, flexible approach is essential to ensure fraud prevention stays effective, responsive, and aligned with organisational goals while minimising disruption.

Managing Different Types of Fraud

Fraud against financial institutions can broadly be split into two categories: high-frequency, low-value fraud and low-frequency, high-value fraud. Both pose significant risks but require tailored approaches to manage effectively.

High-frequency, low-value fraud

This type of fraud is common in day-to-day operations, often involving cards and payments. Examples include small, repeated unauthorised transactions on credit or debit cards and social engineering scams targeting customers through phishing or social media. While individual incidents may involve modest sums, the cumulative impact on resources, customer trust, and operational costs can be significant.

How to tackle it:

- **Technology-Driven Controls:** Use advanced fraud detection systems with adaptable rules and no-code or low-code platforms to respond quickly to new threats.
- **Smart Thresholds:** Balance fraud detection with customer convenience by fine-tuning transaction monitoring and authentication thresholds.
- **Customer Awareness:** Proactively educate customers to recognise scams like phishing or social engineering.

Low-frequency, high-value fraud

This category includes large-scale fraud, such as investment scams or pension fraud, where fraudsters target individuals for significant sums. Examples might include fake investment schemes or convincing customers to transfer savings into fraudulent accounts. The financial and reputational damage from these incidents can be substantial, particularly if the institution is perceived as failing to protect its customers.

How to tackle it:

- **Enhanced monitoring:** Apply stricter scrutiny to high-value transactions, especially those involving unknown entities or overseas accounts.
- **Specialist expertise:** Engage fraud specialists, including those with law enforcement backgrounds, to anticipate and counteract complex scams.
- **Customer protections:** Offer clear policies on victim compensation to maintain trust and meet regulatory requirements.
- **Internal safeguards:** Strengthen controls to prevent misuse of accounts within the institution, such as those used to receive fraudulent funds.

Tailoring a Fraud Strategy to Your Organisation

Your fraud strategy should match your organisation's level of maturity, whether you're starting from scratch or refining a well-established approach.

For organisations new to fraud prevention

If you're just beginning, focus on laying strong foundations:

- **Educate stakeholders:** Ensure decision-makers understand key risks, from APP fraud to card scams, and their broader implications.
- **Identify risks:** Use workshops to explore fraud types, regulatory demands, and the value of a unified strategy.
- **Understand the problem:** Analyse your fraud data to grasp the scale and nature of the issue. Establish metrics for fraud losses, case volumes, and customer impact.
- **Assess capabilities:** Evaluate governance, expertise, and data collection. Are senior leaders engaged? Do you track fraud losses effectively?
- **Set priorities:** Begin with basics like improving fraud monitoring, reporting, and customer awareness.

This approach will clarify your starting point and define next steps, such as hiring fraud specialists or introducing core controls.

For organisations with established fraud frameworks

For more mature organisations, the focus shifts to enhancing alignment and refining strategies:

- **Integrate goals:** Align your fraud strategy with broader objectives like digital transformation or customer experience improvements.
- **Target key and emerging risks:** Focus on high-impact threats, such as investment scams, while maintaining strong day-to-day defences.
- **Evaluate technology:** Ensure tools can adapt to new threats. Consider no-code or low-code options to reduce IT dependence.
- **Deepen expertise:** Use advanced workshops to explore AI-driven detection, fraud thresholds, and enhanced customer education.

A refined strategy should deliver evidence-based recommendations, driving decisions on resources, technology, and governance to stay ahead of emerging challenges.

The Broader Implications of a Fraud Strategy

Fraud doesn't occur in isolation, and a successful fraud strategy requires a holistic approach that influences decisions and processes across the organisation. To ensure its impact:

- **Align with business goals:** Ensure your fraud strategy complements your financial crime framework and supports broader objectives like digital transformation, customer growth, or cost reduction. Misalignment wastes resources and weakens support.
- **Clarify governance:** Fraud management affects compliance, IT, customer service, and more. Coordination between these teams, with clear accountability for decisions and budgets, is critical to avoiding delays and gaps.
- **Identify interdependencies:** Fraud prevention often overlaps with initiatives like customer experience improvements or tech rollouts. Early recognition of these overlaps prevents friction and ensures smooth integration.
- **Focus on practicality:** Assess whether your strategy fits your current operations, considering potential changes to staffing, technology, or processes. Address constraints—budgetary, technical, or cultural—early.
- **Balance risks and benefits:** A strong fraud strategy builds trust and reduces regulatory risk. However, over-prioritising controls can harm customer experience. Aim for a balance that avoids unintended consequences.

By taking an integrated, practical, and balanced approach, your fraud strategy will strengthen the organisation and support its broader goals.

The BeyondFS Approach to Fraud Strategy

At BeyondFS, we help our clients develop fraud strategies that are proven to work in the real world. Here's how our unique combination of expertise, insight, and results sets us apart:

1. **Practical expertise:** We understand the challenges of implementing a strategy in a live environment. Our approach is grounded in operational realities, ensuring strategies are actionable and effective from day one.
2. **Integrated thinking:** Fraud strategies must align with broader financial crime frameworks and business objectives. We ensure this integration, avoiding contradictions or duplication and creating a cohesive plan that fits the bigger picture.
3. **Cross-functional collaboration:** Fraud impacts multiple areas of an organisation. We bring together all relevant stakeholders to ensure alignment and shared accountability, bridging silos for better outcomes.
4. **Proven knowledge:** Our team brings hands-on experience from leading organisations, having tackled everything from high-value scams to everyday card and payment fraud. This depth of knowledge ensures we approach fraud challenges with confidence and credibility.
5. **Pragmatic approach:** We recognise that most organisations are not starting from scratch. We build on existing frameworks and constraints, saving time and avoiding 'analysis paralysis'.
6. **Tailored solutions:** Fraud maturity varies widely between organisations, and we adapt accordingly. Whether building a strategy from the ground up or refining an advanced framework, we ensure our approach suits each client's specific needs.
7. **Evidence-driven prioritisation:** We focus on using metrics and data to identify risks, allocate resources, and justify budgets. For clients lacking robust data, we help establish baselines to improve decision-making.
8. **Future-proofing:** Fraud evolves quickly, and our strategies are designed to keep pace. We incorporate flexibility and resilience to adapt to emerging threats and organisational changes.

Whether you're tackling high-frequency fraud or complex scams, the BeyondFS team can ensure your organisation is prepared for the future with strategies that protect, enable, and deliver measurable impact.

Fraud won't wait—it's imperative to act now. By understanding the evolving landscape, prioritising effectively, and building a flexible, well-integrated fraud strategy, your organisation can stay ahead of threats, safeguard its customers, and strengthen its position in the market. With the right approach and expert guidance, you can navigate fraud's complexities and build resilient defences for the future.

Fraud won't wait—it's imperative to act now. By understanding the evolving landscape, prioritising effectively, and building a flexible, well-integrated fraud strategy, your organisation can stay ahead of threats, safeguard its customers, and strengthen its position in the market. With the right approach and expert guidance, you can navigate fraud's complexities and build resilient defences for the future.

BeyondFS

Contact

BeyondFS
Dawson House, 5 Jewry St, London
EC3N 2EX, United Kingdom

+44 (0)203 637 4117
info@beyondfs.co.uk
beyondfs.co.uk