

Bottomline®

BANK FRAUD READINESS GUIDE

Stronger Payment Fraud Defense. **Without the Heavy Lift.**

A practical guide for banks operating with lean teams, shared responsibilities and growing fraud pressure.

Commercial payments fraud protection without complexity.

Real-time fraud detection and prevention across the full commercial payment lifecycle, from login and user activity to money movement across ACH, wires, RTP, check, and more. Delivered as SaaS with fast time to value and designed to integrate with Bottomline's Digital Banking platform.

START HERE

What Is Putting the Most Pressure on Your Bank?

Your bank may not have a dedicated fraud operation, but it still faces the same fast-moving fraud threats, customer expectations and regulatory scrutiny as much larger institutions. The difference is operating reality: fewer specialists, shared ownership, limited implementation capacity and little room for disruption.

Do the pain points below sound familiar? Go directly to the corresponding chapter to help identify the risk, explore practical next steps and understand the role Payments Fraud Defense can play without requiring a wholesale replacement of your existing fraud tools.

	YOUR PAIN POINT	GO TO
1	Fraud attempts are rising, but our current controls catch risk too late.	**Chapter 1**
2	Our team is stretched, and fraud is one responsibility among many.	**Chapter 2**
3	Fraud signals are fragmented across payment types and digital channels.	**Chapter 3**
4	We need to show regulators and leadership that our controls are keeping pace.	**Chapter 4**
5	We cannot take on a long implementation or unpredictable cost.	**Chapter 5**
6	We want to strengthen what we have, not rip and replace it.	**Chapter 6**

WHO THIS GUIDE IS FOR

Built for Banks Ready to Strengthen Fraud Protection Without Adding Complexity

This guide is written for banks that play an essential role in the communities and commercial markets they serve. These institutions are close enough to their customers to understand risk in context, agile enough to move with purpose and large enough to require sophisticated protection as fraud threats evolve.

The Opportunity

Fraud ownership often brings together fraud, payments, treasury management, operations, risk, compliance and technology. With the right support, those cross-functional perspectives can become an advantage: faster alignment, clearer ownership and stronger protection across the payment journey.

What Banks Like This Need

- **Unified protection** across users, accounts, and payments.
- **A SaaS model** that reduces infrastructure and maintenance burden.
- **Clear evidence** of effectiveness for executives, customers, auditors and examiners.
- **Risk-based controls** that help stop suspicious activity before fraud losses occur.
- **Integration with Bottomline's Digital Banking platform** and complementary connection into current banking and fraud systems.
- **Predictable cost and measurable value** without an enterprise transformation program.

What This Solution Is Not

Payments Fraud Defense is purpose-built for commercial payments fraud prevention. It is not intended to replace every risk, compliance or financial crime control your bank already has in place.

> Its strength is helping your bank improve real-time detection, interdiction and investigation across high-risk payment journeys while complementing existing systems, workflows and governance programs, including integration with Bottomline's Digital Banking platform.

CHAPTER 1

Rising Fraud Pressure with Controls That React Too Late

THE OPERATING REALITY

Fraudsters exploit the assumption that mid-market banks have fewer layers of defense. Meanwhile, faster payment experiences reduce the time available to review suspicious activity. A control that identifies risk after release may support investigation, but it may not prevent loss.

A PRACTICAL RESPONSE

Move detection earlier in the payment journey and introduce precise interdiction at the point where the bank can still act.

How Payments Fraud Defense Helps

Payments Fraud Defense identifies anomalies across payment activity and can automatically hold suspicious, high-risk payments for review. Real-time interdiction gives your bank an opportunity to release verified transactions or block fraudulent ones before funds move.

Measures That Make the Value Visible



EARLIER DETECTION



LOSS AVOIDED



TIME FROM ALERT TO DECISION



LEGITIMATE PAYMENT APPROVAL RATE

Questions to Ask Internally

- **Where does suspicious payment activity** usually become visible today, and is that early enough to prevent loss?
- **Which payment types or customer journeys** create the shortest window for intervention?
- **What controls** can hold, review or stop a risky payment before funds move?
- **What would earlier detection change** for loss prevention, customer impact and operational response?

CHAPTER 2

Lean Teams, Shared Responsibilities and Alert Overload

THE OPERATING REALITY

At a mid-market bank, the fraud analyst may also be a payments specialist, investigator, operations lead or customer escalation point. Adding another queue, interface or tuning burden can weaken adoption even when the underlying technology is strong.

A PRACTICAL RESPONSE

Prioritize the riskiest activity, make decisions explainable and reduce the effort required to investigate each alert.

How Payments Fraud Defense Helps

Built-in analytics, visual link analysis, an Alert Investigation Center and Record and Replay help teams connect users, accounts, transactions and session behavior. The goal is not simply more alerts. It’s faster, better-informed action with less manual reconstruction.

Measures That Make the Value Visible

- Alert volume
- False-positive rate
- Average handling time
- Cases resolved per analyst
- Escalation rate

Questions to Ask Internally

- **Which fraud tasks** consume the most time for shared teams today?
- **Where do analysts** need to leave one system or workflow to gather enough context for a decision?
- **Which alerts** create the most noise, duplicate review or unnecessary escalation?
- **What information** would help the team make faster, more confident decisions without adding headcount?

CHAPTER 3

Fragmented Risk Across Commercial Payments and Channels

THE OPERATING REALITY

Different payment types, digital channels, and customer activities are often monitored through separate tools and workflows, creating operational siloes and fragmented fraud visibility.

A PRACTICAL RESPONSE

Connect transaction, account and user behavior so risk can be evaluated with more context across payment types and channels.

How Payments Fraud Defense Helps

Payments Fraud Defense provides a more unified view of suspicious behavior and supports multi-rail detection and investigation. For banks using Bottomline Digital Banking, it can integrate into the platform to strengthen fraud protection across payment and channel activity, while also complementing existing systems rather than requiring your bank to retire every control before improving coverage.

Measures That Make the Value Visible



CROSS-CHANNEL CASES IDENTIFIED



DUPLICATE ALERTS REDUCED



PAYMENT TYPES COVERED



TIME TO ASSEMBLE EVIDENCE

Questions to Ask Internally

- **Which payment types,** channels or customer activities are monitored separately today?
- **Where do fragmented tools or workflows** make it harder to connect related risk signals?
- **How quickly** can the team assemble a complete picture of user, account and transaction activity?
- **Which cross-channel fraud patterns** could be missed if each payment rail is reviewed in isolation?

CHAPTER 4

Regulatory Pressure Without a Larger Compliance Staff

THE OPERATING REALITY

Examiners and auditors increasingly expect banks to demonstrate that risk assessments, monitoring, controls, escalation and governance remain appropriate as payment activity changes. The 2025 interagency request for information on payments fraud specifically addressed check, ACH, wire and instant payments fraud and applied to all FDIC-supervised institutions.

A PRACTICAL RESPONSE

Show that controls are risk-based, adaptable, tested and supported by clear evidence. Document how suspicious payments are detected, held, investigated, resolved and tuned.

How Payments Fraud Defense Helps

Configurable fraud risk indicators, investigation evidence, session replay and decision records can support a more defensible control narrative. Payments Fraud Defense strengthens payments fraud controls, but does not replace the your bank's broader compliance, BSA/AML or governance obligations.

Measures That Make the Value Visible

- Control coverage
- Documented tuning
- Investigation evidence
- Exception aging
- Audit findings
- Remediation status

Questions to Ask Internally

- **What evidence can we provide today** to show that payment fraud controls are working as intended?
- **How do we document** control coverage, tuning decisions, exceptions and remediation activity?
- **Where would an examiner or auditor ask** for clearer proof of monitoring, escalation or governance?
- **How can fraud operations support** a stronger control narrative without adding compliance burden?

CHAPTER 5

The Need for Fast Value and Predictable Effort

THE OPERATING REALITY

A technically strong fraud solution can still fail the business case if it requires a multi-year program, scarce specialists or a major infrastructure build. Mid-market banks need confidence in implementation scope, integration effort, pricing and the path to measurable results.

A PRACTICAL RESPONSE

Define a phased use case, establish baseline metrics and prioritize the highest-risk payment journeys first.

How Payments Fraud Defense Helps

Payments Fraud Defense is delivered in Bottomline's secure, regulated proprietary cloud and is positioned for rapid deployment. This fraud solution can deliver measurable value within weeks, helping banks like yours modernize controls without taking on enterprise-scale infrastructure.

Measures That Make the Value Visible

- Time to launch
- Integration milestones
- First use case live
- Fraud-loss trend
- Manual review reduction
- Total operating cost

Questions to Ask Internally

- **Which high-risk use case** could deliver measurable value first?
- **How will we define success** before deployment so value is visible within the first weeks?
- **What data, integration steps and internal resources** would be required for an initial phase?
- **What cost, timeline or scope questions** need to be answered before stakeholders can align?

CHAPTER 6

Strengthening Existing Controls Without Rip and Replace

THE OPERATING REALITY

Your bank, like many others, are not starting from zero. You already have core controls, online banking protections, payment rules and established workflows. The need is to close gaps created by rising or emerging fraud, faster payments and fragmented insight without destabilizing what works.

A PRACTICAL RESPONSE

Augment the existing environment. Add earlier detection, broader behavioral insight and real-time interdiction where current controls need reinforcement.

How Payments Fraud Defense Helps

Bottomline positions Payments Fraud Defense to complement your existing fraud systems and integrate with Bottomline's Digital Banking platform. Flexible integration and configurable detection allow your bank to focus on priority gaps while preserving current investments and workflows.

Measures That Make the Value Visible

- Existing tools retained
- Incremental coverage
- Implementation disruption
- Adoption by current teams
- Value from avoided replacement

Questions to Ask Internally

- **Which current controls,** systems and workflows must remain in place?
- **Where do existing tools need added visibility,** earlier detection or stronger interdiction?
- **How can we close priority gaps** without disrupting teams, customers or downstream processes?
- **What evidence would show** that augmentation is delivering value without unnecessary replacement?

WHY BOTTOMLINE

Proof That Reduces Perceived Implementation Risk

For a lean bank, vendor proof is not only about scale. It's about confidence that the provider understands business payments, can support a regulated operating environment and can help show value without creating a new layer of complexity.

35+ years — Payments Experience

500+ — Commercial Fraud and Compliance Customers

$16 trillion — Payments Moved Annually

92 countries — Coverage Across Six Continents

1 million — Businesses Using Bottomline

Within weeks — Bottomline-Stated Path to Measurable Value for Payments Fraud Defense

What the Technology Contributes

- Real-time detection and interdiction for suspicious payments.
- Behavioral analytics and AI-enabled detection designed to improve precision.
- Visual link analysis to connect users, accounts and transactions.
- Record and Replay to reconstruct end-user activity without relying only on log files.
- Configurable risk indicators that can adapt as threats and regulatory expectations change.
- A cloud delivery model designed to reduce infrastructure burden.

ACTION PLAN

A Low-Lift Path from Concern to Control



Select the Pressure Point

Select the highest-priority fraud pressure point from the guide and confirm the chapter that best matches the bank's current challenge.



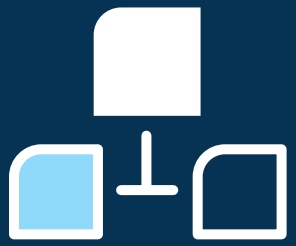
Establish a Baseline

Document baseline metrics, including current fraud attempts, losses avoided or incurred, alert volume, handling time, payment coverage and control gaps.



Choose One High-Value Use Case

Identify one high-value payment journey or use case where loss exposure, customer impact, review burden, earlier detection, better context and real-time interdiction could deliver measurable impact.



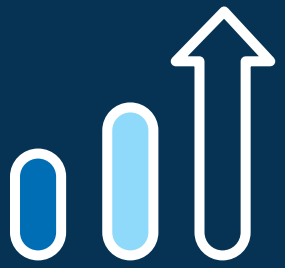
Map the Workflow

Map the current workflow across data sources, decision points, owners, escalation paths and payment hold, release or block steps. Assess where existing tools need added visibility, cross-channel context or stronger interdiction without requiring rip and replace.



Define Success Before Deployment

Define success measures before deployment, including launch timeline, false-positive reduction, average handling time, cases resolved, loss avoided, audit-ready evidence, stakeholder alignment and a reporting cadence to track outcomes, tune controls and document progress.



Expand Based on Evidence

Plan the next expansion phase based on evidence from the first use case, adding payment types, channels or detection strategies as value is proven and implementation requirements, integration dependencies, resource needs and expected time to value are understood.

NEXT STEP

Protect More Payments Without Building a New Enterprise Fraud

Payments Fraud Defense helps banks add real-time detection, money movement controls and investigation capabilities across payment types and digital channels. Designed to integrate with Bottomline's Digital Banking platform, the solution complements existing controls, supports lean teams and accelerates value through SaaS delivery.



Start With Your Highest-Priority Pain Point

If your checklist reveals gaps in your payment fraud workflow, you do not have to close them alone. **Contact us** to request a working session where we can help map your high-risk payment journeys, identify operational gaps, and define practical next steps to strengthen protection.

Let's Chat

Important: This guide is marketing content and does not constitute legal, regulatory or compliance advice. Banks should validate requirements with their legal, compliance, risk and supervisory stakeholders. Product capabilities and implementation timing should be confirmed for the bank's specific environment.

Bottomline

REV US110626KH

© Copyright 2015 - 2026 Bottomline Technologies, Inc. All rights reserved.

Bottomline, Paymode, and the Bottomline logo are trademarks or registered trademarks of Bottomline Technologies, Inc. All other trademarks, brand names or logos are the property of their respective owners.

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1 603-436-0700
Toll-free: +1 800-243-2528
info@bottomline.com