

Protect Payments Across Applications,
Channels, and Payment Types

Bottomline Cyber Fraud & Risk Management: Secure Payments

Bottomline Technologies' Cyber Fraud and Risk Management (CFRM) enables corporations and financial institutions to reduce risk, prevent fraud, and meet regulatory compliance requirements through a highly extensible and flexible platform that delivers unparalleled fraud protection.

CFRM is an innovative end-to-end enterprise fraud management solution suite that includes a unique combination of comprehensive data capture methods combined with cross-channel analytics and real-time alerting. This allows organizations to detect and prevent internal and external fraud in real-time and to better manage compliance requirements related to fraud incidents.

Bottomline's CFRM platform is highly extensible and flexible with a rapid activation model so organizations can quickly achieve:

- Better visibility & control
- Faster investigations
- Quicker decision making

The platform layers intelligent machine learning, rules-based detection, and behavioral profiling for anomaly detection and monitoring of end-user activity and transactions across applications and channels throughout the entire enterprise. The system tracks all end-user activity in multiple environments from mainframe to web, to mobile and in-house and 3rd-party solutions.

CFRM Solutions:

SECURE PAYMENTS

- ⊕ • Applications
- Channels
- Payment Types

COMPLIANCE

- ⊕ • Anti-Money Laundering
- Sanctions Screening
- Know Your Customer
- Enterprise Case Management

USER BEHAVIOR ANALYTICS

- ⊕ • Insider Threat Detection
- Intruder Detection

Key CFRM Platform Features

Real-Time Suspicious Transaction Interdiction – With the growth of Same-Day ACH and wire transfers, real-time monitoring, alerting and transaction blocking (interdiction) are essential components of the solution. When suspicious transactions or conditions are detected, transactions can be automatically quarantined until explicitly released by an authorized investigator or payments specialist. In addition, if the suspicious activity is not related to a specific transaction but occurs during an online or mobile session, then step-up authentication can be triggered prompting the user to respond before proceeding with risky activity. CFRM can also send notifications to other authentication systems to trigger out-of-band authentication or one-time passwords.

Fraud Analytics with Intelligent Machine Learning – By layering supervised and unsupervised machine learning with rules based detection and behavioral profiling, CFRM constantly enhances its analytics engine and incorporates real-time adaptive intelligence into fraud detection. Leveraging Bottomline's deep expertise in payments and fraud, the CFRM analytics engine uses intelligent machine learning to enable organizations to stay ahead of evolving and complex fraud schemes, reduce false positives, and protect their payments. This is combined with rules based detection and behavioral profiling in order to quickly protect against known fraudulent behaviors and attacks on low volume transaction types.

Cross-Channel Behavior Tracking – The behavior of customers, accounts, employees and other entities is tracked and profiled by the analytics engine which correlates activities between various channels such as e-Banking, mobile, ACH, wires, checks, call center and others and generates real-time alerts on suspicious or anomalous events.

Investigations and Case Management – Suspicious events can be investigated in the Investigation Center, a powerful forensics web-based user-interface, allowing investigators to manage and document the investigation process, view all information relevant to alerts, cases or profiles, in one consolidated view with flexible drilldown options on each related entity.

Visual Replay – The system non-invasively, and without an agent, captures a detailed audit trail allowing complete visibility into end-user activity with visual replay of every screen, user modifications, and flow of screens in core business applications. The system also provides Google-like search capability on the content of every user screen and session, enabling investigators to immediately get answers to questions such as: which user accessed a specific account number in a given timeframe, and then replay the exact activities of the user screen-by-screen. This functionality enables compliance with GLBA, SOX, PCI and other regulations that require a detailed audit trail of access to sensitive customer data.

CFRM Platform





Secure Payments Module

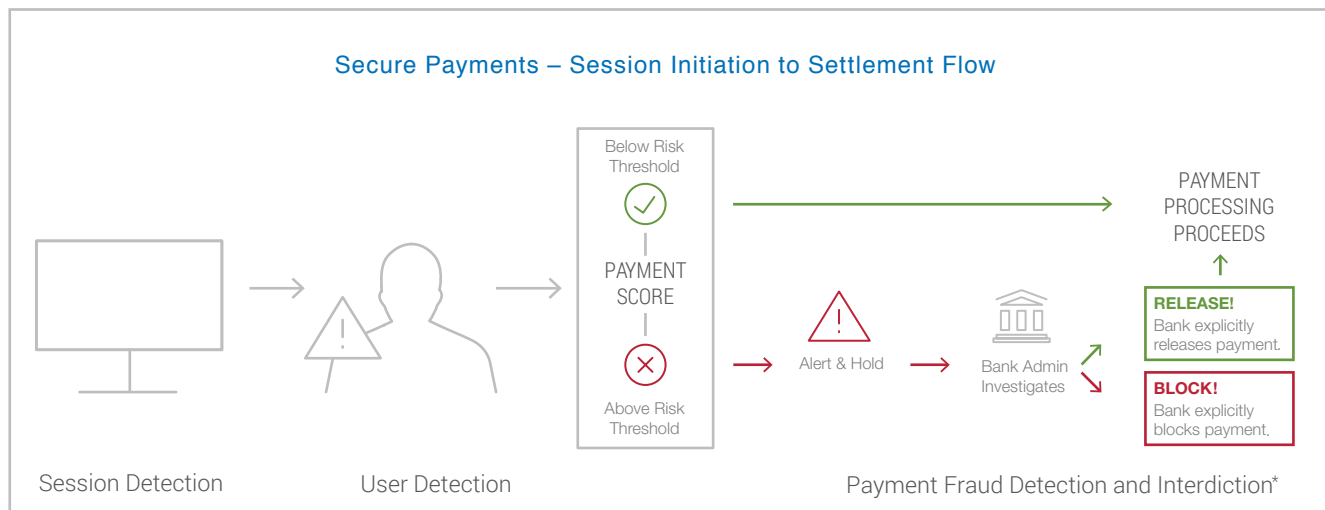
Bottomline's Secure Payments solution protects payments across a variety of applications, channels and payment types. With Secure Payments from Bottomline, your organization can:

- Detect fraudulent payments in real-time
- Block payments prior to release
- Secure online and mobile sessions and account activity
- Cover all your payment types and channels within a single enterprise solution
- Meet regulatory compliance needs

Through an out-of-the-box library of pre-built integrations and support for diverse payment formats, Secure Payments provides on-going flexibility for comprehensive behavioral analytics, real-time alerting, and transaction blocking, allowing your organization to reduce risk, prevent fraud and meet regulatory compliance needs.

APPLICATIONS	CHANNELS		PAYMENT TYPES	
Banking Platforms	POS	Branch	ACH	ISO 8583
Payment Hubs	Online	Call Center	BACS	SEPA
Service Bureaus	Portals	Host2Host	Bill Pay	SIC4
TMS	Mobile	IVR	Check	SWIFT
ERPs	ATM		ISO 20022	Wire

Bottomline's Secure Payments solution effectively identifies and mitigates some of today's most sophisticated fraud schemes, such as Business Email Compromise (BEC) and cross-channel attacks.



*This can work independently of Session and User Detection in the absence of online activity.

Connect with us



© Copyright 2018. Bottomline Technologies, Inc.
All rights reserved. Bottomline Technologies and the BT logo is a trademark of Bottomline Technologies, Inc. and may be registered in certain jurisdictions. All other brand/product names are the property of their respective holders. REV 062818

Corporate Headquarters

325 Corporate Drive, Portsmouth,
NH 03801, United States of America

Phone: +1 603.436.0700
Toll-free: +1 800.243.2528
Fax: +1 603.436.0300
info@bottomline.com