Bottomline

Insider and Employee Fraud

Bottomline's CFRM Solution Overview

Bottomline Technologies' Cyber Fraud and Risk Management (CFRM) suite of solutions is an innovative end-to-end enterprise fraud management solution which provides a unique combination of comprehensive data capture combined with cross channel analytics and real-time alerting. This allows organisations to reduce risk, prevent fraud and meet regulatory compliance requirements through a highly extensible and flexible platform that delivers unparalleled fraud protection.

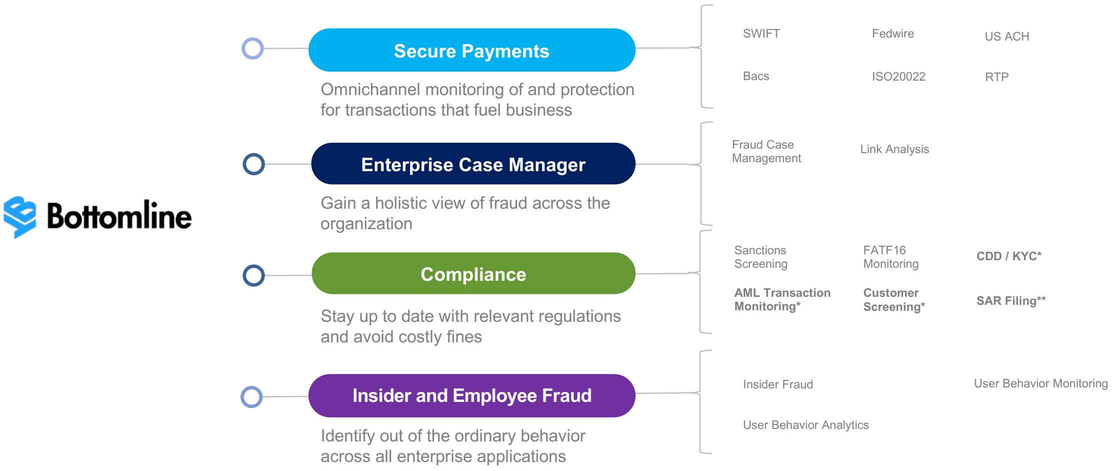
The CFRM platform is designed in a modular way that enables frictionless deployment of new functionality in order to meet varying use cases. The primary solutions within the CFRM platform are:

SECURE PAYMENTS – Bottomline's Secure Payments solution protects payments across a variety of applications, channels, and payment types. Whether it is one business critical application, channel and payment type, or a variety, our highly flexible and extensible platform delivers proven protection against payment fraud through advanced analytics of user behavior and transaction flows layered with intelligent machine learning, reducing risk for some of the largest corporations and financial institutions in the world.

ENTERPRISE CASE MANAGER – Bottomline's Enterprise Case Manager solution is designed to simplify and streamline the risk management and fraud detection process, along with the various regulatory processes that accompany these efforts. The solution integrates across multiple systems and enables users to track all alerts and cases regardless of their source application. When violations are found, the system helps to automate the filing of Suspicious Activity Reports (SARs) to government agencies.

COMPLIANCE – Bottomline's Compliance solution provides corporations and financial institutions with a powerful end-to-end offering to accelerate the speed to achieve regulatory compliance requirements while decreasing complexity. Whether the need is around modernising an anti-money laundering program, achieving more reliable sanctions screening, improving payments monitoring, highlighting settlement exposure, or automating suspicious activity reporting to meet regulatory requirements, Bottomline's Compliance solution offers a modular approach to reducing the cost of compliance and increasing productivity.

INSIDER AND EMPLOYEE FRAUD – Bottomline's Insider and Employee Fraud solution quickly identifies and stops anomalous user activity through intelligent machine learning, rules-based detection, and years of experience protecting some of the largest corporations and financial institutions in the world. The solution captures all user behavior in real-time across all vital systems and provides protection for both external threats in which user credentials have been compromised and internal threats from authorised users.


Bottomline
Secure Payments
Omnichannel monitoring of and protection for transactions that fuel business
SWIFT
Fedwire
US ACH
Bacs
ISO20022
RTP
Enterprise Case Manager
Gain a holistic view of fraud across the organization
Fraud Case Management
Link Analysis
Compliance
Stay up to date with relevant regulations and avoid costly fines
Sanctions Screening
FATF16 Monitoring
CDD / KYC*
AML Transaction Monitoring*
Customer Screening*
SAR Filing**
Insider and Employee Fraud
Identify out of the ordinary behavior across all enterprise applications
Insider Fraud
User Behavior Monitoring
User Behavior Analytics

Introduction to Insider and Employee Fraud

The Insider and Employee Fraud product is a pre-packaged solution suite designed for financial institutions. It is specifically designed to identify and track suspicious employee activity by monitoring each action a user makes and analyzing those actions for unusual behavior and key risk indicators. When an employee action or pattern of actions are deemed by the analytics as potentially fraudulent, an alert is created for compliance officers to review and investigate. These analytics take a variety of different factors and data points into account and because the system monitors real-time actions, as well as historical data, it can capture a variety of different fraud schemes while reducing false positives.

EVALUATING USER BEHAVIOR FOR FRAUD AND RISK INDICATORS

As the system monitors employee behavior, it builds an understanding of what is normal for each specific employee and how their behavior compares to that of their peers. This helps to surface suspicious activity without introducing unnecessary false positives. For example, if one employee is designated to only work with VIP accounts you would not want alerts going off every time that employee accessed a VIP account. Instead the system would learn that this is a false positive and add that to its understanding of what is normal for that user. Similarly, this process can be used to identify suspicious behavior. For instance, if a user normally looks at a few records a day but then begins viewing a significantly higher volume of records this could be flagged as suspicious activity for a compliance officer to investigate.

The solution's analytics have been refined over years of experience working to prevent insider and employee fraud across multiple instances. As a result, the solution is able to identify over 100 different scenarios that have been proven to indicate insider fraud activities. Bottomline is able to work with customers to tune the analytics to help focus on the scenarios that are deemed most important with each implementation.

All alerts generated by the system are displayed in the Investigation Center where they can be tracked and managed by compliance officers. Alerts contain the critical data such as the details of the scenario that triggered the alert. The alert also provides additional information such as previously related alerts and other historical data that could be useful for the investigator. This combination of information provides all the relevant information required to begin the investigation process and quickly come to a resolution.

The solution is able to identify over 100 different scenarios that have been proven to indicate insider fraud activities.

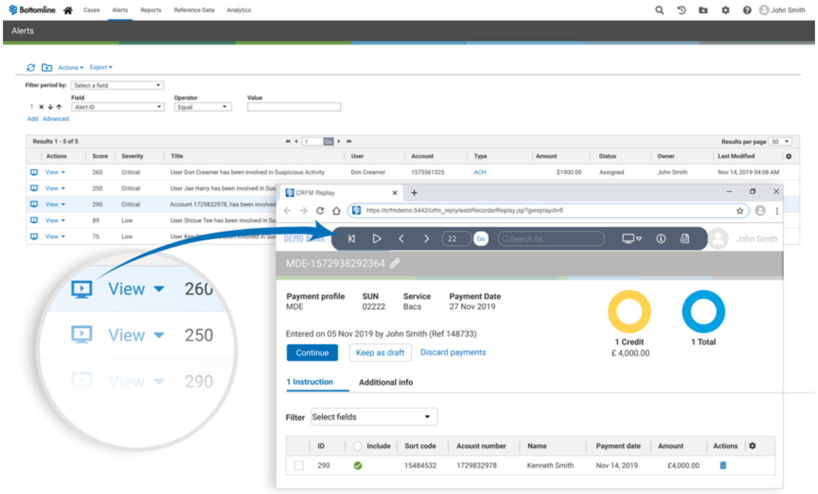
Web Application End-User Session Replay

Investigation Workflow

The solution can capture user data through a variety of methods including APIs, MQ, network sniffing, and log capture. As data is gathered from the monitored application, it is passed to the analytics engine for evaluation. This evaluation can be performed in real-time or through an overnight batch process depending on the scenario and solution deployment. If the solution deems any user activity to be a policy violation or generally suspicious, then an alert is generated and an email is sent to the assigned investigators for further evaluation.

Investigators can use a wide range of tools to understand why the alert was generated. These tools include:

- **Screen-by-screen replay*:** Investigators can replay the exact screens the user saw and the actions they took including view-only actions which are not captured in many audit logs. This provides powerful forensic evidence for understanding why an action was taken and if it was legitimate.



Filter period by: Select a field

Field: Alert ID | Operator: Equal | Value:

Results 1 - 5 of 5 | Results per page 50

Actions	Score	Severity	Title	User	Account	Type	Amount	Status	Owner	Last Modified
View	260	Critical	User Don Creamer has been involved in Suspicious Activity	Don Creamer	1575561325	ACH	$1900.00	Assigned	John Smith	Nov 14, 2019 04:08 AM
View	250	Critical	User Jae Harry has been involved in Sus							
View	290	Critical	Account 1729832978, has been involved							
View	89	Low	User Shizue Tee has been involved in Su							
View	75	Low	User Ken							

https://crfmdemo:5442/crfm_reply/webRecorderReplay.jsp?gxreplayid=6

MDE-1572938292364

Payment profile: MDE | SUN: 02222 | Service: Bacs | Payment Date: 27 Nov 2019

Entered on 05 Nov 2019 by John Smith (Ref 148733)

1 Credit £ 4,000.00 | 1 Total

Filter: Select fields

	ID	Include	Sort code	Acount number	Name	Payment date	Amount	Actions
□	290	✓	15484532	1729832978	Kenneth Smith	Nov 14, 2019	£4,000.00	

- **Cross-platform search:** The cross-platform search allows investigators the ability to search any term across any monitored application. For example, to find all users who accessed a specific customer account within a specific timeframe. This search can be easily performed on recorded data from a specific platform or on data recorded from several platforms.

- **Reports:** The solution is able to report on myriad data including user actions, generated alerts and any other data related to defined entities in the system. A number of pre-configured reports are available to go along with a robust custom reporting engine.

At this point, the investigator can choose how to best resolve the alert by marking it as False Positive, Justified (meaning the alert is legitimate, but not valid in this particular case) or Fraud. If further investigation is required in order to determine the cause of the fraudulent or suspicious event, the users can take advantage of the Case Management functionality within the Investigation Center. Further information Enterprise Case Management is available.

*Dependent on method of data capture

Insider and Employee Fraud Analytics

The analytics engine provides a data model which supports advanced calculations and correlations in real-time. The data model can maintain static and dynamic information on various types of entities including employees, accounts, customers and others.

The data captured by the system from various sources is sent to the analytics engine in a normalised way, so the data can be captured in a way that is transparent to the analytics engine.

Our analytics engine uses a layered approach that looks at past data trends while continuously identifying new anomalies within the data and incorporating investigator feedback into its evaluation criteria. This approach enables customers to get immediate time to value by detecting known bad behaviors while also continuously adapting to emerging threats and refining risk scoring to reduce false positives.

HOW THE ANALYTICS WORK

During initial implementation and onboarding, pre-configured analytics are deployed based on the use cases under consideration by the customer. These analytics are based on the library of scenarios available within the Insider and Employee Fraud solution or can be configured on a custom, case-by-case basis as needed. For some use cases, this enables the solution to immediately begin identifying high-risk behavior. This is typically able to occur with more binary use cases, such as policy violations.

In parallel, as the system begins to monitor user behavior it also begins to understand what is normal for employees. As these baselines are established, the solution will begin to raise incidents on a wider range of scenarios. This could include a user performing action more often than they typically do within a work day or a user performing an activity that is not typically performed by someone with their same role.

MACHINE LEARNING

In addition to identifying known scenarios and anomalous behaviors, Bottomline's Cyber Fraud and Risk Management solutions incorporate machine learning to further refine their analytical capabilities and increase fraud detection capabilities. The solutions utilise supervised and unsupervised learning techniques in order to maximise the analytic capabilities of the solution. Machine learning enables the analytics engine to discover previously unknown anomalies, reduce false positives and continuously refine the analytics based on user interaction with the generated alerts.

These machine learning capabilities are particularly effective as they leverage the depth of fraud detection expertise that the solution provides. All machine learning algorithms are built to leverage expert defined features within the data while also building in insights from the high-risk behavior and policy violations identified by the standard analytics engine. By leveraging these data points, Cyber Fraud and Risk Management is able to provide more insightful and meaningful results for compliance officers.

Solution Use Cases

The Insider and Employee Fraud solution can be deployed across different channels and applications. Customers can elect to deploy a single use case or multiple and all user activity is aggregated into the same Investigation Center for a consistent user experience and streamlined investigations. The following use cases represent a sample of the types of scenarios that the Insider and Employee Fraud solution is capable of identifying for customers. All use cases are refined through the incorporation of machine learning as supervised models improve risk scoring models in the analytics and combine with new outliers found through unsupervised learning.

LEAKAGE OF SENSITIVE INFORMATION/DATA THEFT

- Performing account/customer inquiries, above the average expected number
- Performing an excessive number of account/customer prints
- Performing an excessive number of common name searches
- Performing an excessive number of detailed inquiries without subsequent monetary transaction
- Behaving inappropriately for a given role (e.g., off-hours inquiries, examining other departments' accounts, inquiring on accounts from other states/regions/countries)
- Performing a customer inquiry on a customer who belongs to a VIP active list
- Downloading large amounts of information

EMBEZZLEMENT

- Account has monetary transaction(s) of a certain category with a large total amount
- Account with excessive transactions of a certain category
- Branch has excessive number of transactions of a certain category on accounts of a certain type
- Employee own account has an excessive number of transactions of a certain category
- Employee performs a monetary transaction on an account which doesn't have any recent activities
- Employee performs withdrawals from escheatable accounts

INTERNAL ACCOUNT TAKEOVER

- Account is logged in multiple times from multiple different IP addresses at once
- Logging in from new IP address
- Logged in from an implausible geo-location based on last login time and place
- Deviation from normal working behaviors (e.g., off-hours inquiries, examining other departments' accounts, inquiring on accounts from other states/regions/countries)
- Employee logged in without swiping badge

POLICY VIOLATIONS

- Accessing accounts of coworkers
- Opening a multiple number of low or no balance accounts
- Performing a customer inquiry on a customer who belongs to a VIP active list
- Performing excessive number of refund transactions over the last 7 days
- Performing a money transfer(s) on their own account
- Performing fee reversal(s) on their own account
- Performing account/customer inquiries, above the average expected number
- Performing a service transaction on their own account

About Bottomline

Bottomline (NASDAQ: EPAY) makes complex business payments simple, smart and secure. Corporations and banks rely on Bottomline for domestic and international payments, efficient cash management, automated workflows for payment processing and bill review, and state of the art fraud detection, behavioral analytics and regulatory compliance solutions. Thousands of corporations around the world benefit from Bottomline solutions. Headquartered in Portsmouth, NH, Bottomline delights customers through offices across the U.S., Europe, and Asia-Pacific.

For more information, visit **www.bottomline.com**

Bottomline

Connect with us

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

Europe, Middle East, Africa Headquarters
1600 Arlington Business Park
Theale, Reading, Berkshire RG7 4SA
United Kingdom

Tel (Local): 0870-081-8250
Tel (Int): +44-118-925-8250
Fax: +44-118-982-2253
emea-info@bottomline.com

Asia Pacific Headquarters
Level 3, 69-71 Edward Street
Pyrmont, Sydney NSW 2009
Australia

Tel: +61-2-8047-3700
Fax: +61-3-9824-6866
apac-info@bottomline.com