<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>The Cyber Fraud Challenge</td>
</tr>
<tr>
<td>05</td>
<td>Bottomline User Behavior Monitoring</td>
</tr>
<tr>
<td>08</td>
<td>Bottomline Enterprise Case Manager</td>
</tr>
<tr>
<td>11</td>
<td>Bottomline Insider Fraud</td>
</tr>
<tr>
<td>14</td>
<td>Bottomline Check Fraud</td>
</tr>
<tr>
<td>17</td>
<td>Bottomline Web Fraud and Security</td>
</tr>
<tr>
<td>20</td>
<td>Bottomline Sanctions Screening</td>
</tr>
<tr>
<td>23</td>
<td>Case Study</td>
</tr>
</tbody>
</table>
The Cyber Fraud Challenge

The number of cyber fraud attacks and the resulting costs are skyrocketing.

Attackers, whether inside or outside your organization, are using more sophisticated techniques to gain access to sensitive information. Additionally, the evolved fraud tactics being used are more difficult for traditional security systems to identify. In order to protect both corporate and customer data, decision makers must rethink how they approach fraud detection and overall cyber security. Your financial institution needs complete visibility into user behavior. Without it, you’re missing a critical line of defense.

You’re only as productive as your tools allow you to be.

Traditional, siloed, and rigid solutions lack the technical sophistication to ward off hordes of fraudsters who are constantly evolving their methods of subterfuge. Unless you adapt, your company is at risk.
The key to protecting your financial institution is in the strategy that defines the tools you employ. More than collect and analyze, you need to be equipped with the visibility and intelligence necessary to act.

Leveraging Intellinx technology, Bottomline Technologies’ Cyber Fraud and Risk Management solutions provide cutting-edge tools to noninvasively monitor and analyze user activity, alert, and resolve fraud before and as it happens, and all from within one dashboard. Going beyond log files capturing user behavior activity as the attacker breaches, Bottomline solutions aid in reducing fraud and ensuring regulatory compliance, and do so quickly.

Rethink your cyber fraud strategy.

$20.8 million: The average data breach cost at financial organizations.

US Dept of Justice, 2013
You can’t stop fraud if you don’t know what your users are doing.

Most security investments protect financial institutions from malware and the risks of unauthorized access—but it isn’t enough.

Many financial institutions have an incomplete picture of what their authorized users are doing, creating a critical blind spot when it comes to detecting and stopping fraud.

Tracking activities isn’t enough. Track behavior, too.

A user’s activity may appear normal in one system, but abnormal in another. How can you tell the difference? Cross-channel technology that analyzes patterns of behavior across networks, applications, and over time can help you spot—and stop—suspicious activity in real time.

- Track behavior instead of individual transactions.
- Act on suspicious behavior before damage is done.
- Increase organizational security with centralized visibility.
Log files aren’t enough.

System-generated audit logs are expensive, time-consuming to analyze, and only tell one part of the story, often much too late. This challenge can be alleviated through the investment in one central system of record.

Protect your financial institution with a “virtual surveillance camera.”

Bottomline User Behavior Monitoring is a patented and non-invasive solution that sniffs the network traffic between users, systems, and applications—analyzing live exchanges and reconstructing complete user sessions.

It’s like having a surveillance camera that provides a screen-by-screen replay of everything users see and do across systems and applications. The solution won’t impact network or system performance.

49%: Percentage of respondents who agreed that log collection and analysis is not effective in identifying application users who misuse sensitive or confidential information.

How it Works:

Bottomline User Behavior Monitoring incorporates Intellinx technology to flag the unusual activity of authorized users. For example, if an employee accesses files unrelated to their job multiple times within a given period, investigators can replay all of the employee’s interactions—every screen and every click—to detect potentially fraudulent activity.

Features Include:

- **Real-Time Alerts & Investigations of Alerts & Cases:** Precisely investigate alerts and document suspicious behavior in the case system in real-time.

- **Powerful Reporting Function:** Generate reports for any type of access, which can be filtered and sorted.

- **Link Analysis:** Visually display relationships between users (employees, customers, accounts, and others), systems, and data. Fraudulent entities, or those under investigation, are highlighted to allow further examination.

- **Screen-by-Screen Replay:** Investigators can replay user activity and analyze behavior, screen for screen, to fully understand everything that a user did and saw across systems and applications over time.

- **Cross-Platform Search of User Activity:** Perform a Google-like search on the content of all screens accessed by users across disparate systems in a given timeline, to find, for example, all users who accessed a specific customer account in a specific timeframe.
Bottomline Enterprise Case Manager

Time is of the essence.

Stopping fraud in real time is a challenge when you’re relying on manual log file review and analysis.

Dated technology isn’t adaptable.

While fraud is becoming increasingly more dynamic and sophisticated, most traditional solutions are unable to keep pace with changes in threat types and to provide the agility needed for real-time investigations.
Limited protection will leave you vulnerable.

A solution that fails to protect your entire enterprise will increase your exposure to fraud. Ensuring that your organization complies with government regulations and files Suspicious Activity Reports (SARs) in a timely manner should be a minimum requirement.

Protect your financial institution with an end-to-end case management system.

Bottomline Enterprise Case Manager is a central hub—empowering investigators with a scalable, company-wide alert and case management system that reduces financial risk and offers cost-effective regulatory compliance. Seamless to integrate and easy to configure, this robust option can replace siloed, obsolete, or homegrown systems.

54%: Percentage of companies that say it is difficult to identify application user activities that are illegal or inappropriate in real time.

Give investigators a centralized console to manage all cases.

Speed investigation times and increase productivity.

Easily estimate the financial impact of suspicious activity.

How it Works:

Bottomline Enterprise Case Manager detects suspicious activity and provides the management visibility needed to support changes to your business. It automatically identifies for which case a SAR should be filed and generates the SAR in the FINCEN-required format for electronic filing. The system gives investigators all of the tools and information needed to handle and resolve the case—without exhausting the resources of your fraud and compliance teams.

Features Include:

**Comprehensive Case Management:**
In the case of a red flag, the platform gathers all necessary information from relevant sources. From the central hub, investigators are provided a cross-channel view of suspicious activity.

**Single System of Record:**
Because it’s connected to all relevant corporate systems and data sources, Enterprise Case Manager reduces redundancy and provides a single data source for investigators.

**Financial Impact Calculator:**
Looking into financial exposure, anticipated loss, and pre-charge of recoveries, Enterprise Case Manager automatically estimates the financial risk of suspicious activity and suspected fraud.

**Fully Adaptable:**
Enterprise Case Manager helps compliance departments manage workload and optimize productivity. It’s completely scalable, packaged with preconfigured reports, dashboards, and workflows, which eliminate the need for programming or IT support.

**A Suite of Reporting Capabilities:**
Automatically identifying the need to file a SAR, Enterprise Case Manager improves compliance with government regulations and assists in its creation.

*Enterprise Case Manager automatically:*
- Notifies when a SAR is required.
- Alerts when a deadline is approaching.
- Populates the deadlines, reducing the chances of overlooking an SAR, or filing it too late.
Information leaks jeopardize relationships.

The inability to effectively monitor exactly what users are doing can open the doors to data leaks, loss of reputation, and shareholder value.

Invest in a true end-to-end fraud solution.

Bottomline Insider Fraud provides a level of unmatched insight: full visibility into user behavior. This not only helps stop fraud in its tracks, it has the power to deter potential fraudsters by detecting unusual activity and behavior as well as creating total employee accountability.
Stop malicious insiders now.

Distinguishing between malicious, negligent, and ordinary activity when every employee uses the same legitimate system commands is a complex process.

An anti-fraud solution shouldn’t be one-dimensional.

Fraudulent behavior is difficult to track across disparate systems—you simply cannot rely on a partial picture of user activity

- Eliminate time-consuming log file reviews.
- Maintain complete visibility into user behavior.
- Respond immediately to new threats.

78% of occupational fraud is committed by or with employees.

$3.7 trillion: Global insider fraud loss in 2014.

How it Works:

Using the knowledge from more than 200 deployments, and the experience of the Intellinx staff, the pre-packaged library of rules has been refined to detect anomalies in work patterns and data. It’s easy to set up, and the rules are easily configurable to the risk scenarios specific to your organization.

Examples of Rules:

**Rule:** Leakage of sensitive information
**Alert:** User performs account or customer inquiries that are above the average expected number.

**Rule:** Embezzlement
**Alert:** Monetary transaction(s) of a certain category with a large total amount are attempted.

**Rule:** Policy violations
**Alert:** The creation of multiple low-or no-balance accounts is detected.
Despite declining check volumes in the banking industry, losses attributed to check fraud are still among the highest of any fraud type.

Fraud schemes are on the rise.

Rigid systems lack flexibility.

Fraudsters are using new, sophisticated methods through multiple channels and cutting-edge technologies. Your risk solution should be just as sophisticated and agile.
Bottomline Check Fraud provides cross-channel analytics that can help detect a wide variety of check fraud schemes including deposit fraud, on-us fraud, and check kiting. This system tracks activity across multiple accounts of the same customer and detects all links between accounts and customers.

**Profiles** customer accounts to detect deviations and suspicious activity.

**Assesses** every possible connection between accounts and customers.

**Tracks** activity across multiple accounts of the same customer.

**Reduces** false positives using predictive modeling.

**Collects** and stores extensive data in a single source for investigations.

Among organizations that experienced attempted or actual fraud, 82% were victims of check fraud.

2014 AFP Payments Fraud and Control Survey

- Detect and respond to a wide variety of check fraud schemes.
- Gain visibility into activity across accounts and connections between accounts and customers.
- Easy integration with check imaging, items processing, and DDA systems.
How it Works:

Using rules and user profiles, each transaction is assigned an overall fraud risk score. If the risk score crosses a predetermined threshold, an administrator is prompted to make a pay or no-pay decision. Extensive information is captured, including the front and back of check images, and is presented when an alert is triggered and displayed to the investigator. All alerts are housed in the Investigation Center to ensure rapid decisions are made and to streamline investigation follow-up.

Examples of Rules:

**Rule:**
*Deposit fraud*

**Alert:**
A user makes an unusually large check deposit.

There has been an excessive amount of daily monetary check deposit amounts.

**Rule:**
*On-us fraud*

**Alert:**
The system detects that multiple on-us check transactions of the same amount were made.

**Rule:**
*Check kiting*

**Alert:**
There are multiple check transactions of the same amount.

Excessive return deposit transactions are made.
Without analytics, compromised accounts will go under the radar.

Most solutions don’t monitor all layers of web traffic and user actions—and ultimately cannot tell if a customer’s account has been compromised.

Protect your financial institution’s online customer base.

Bottomline Web Fraud and Security is designed to identify and prevent fraud on your institution’s external, online platform. By monitoring all web traffic, analyzing it, and alerting investigators to suspicious activity, this solution helps stop fraudulent activity. It also learns and adapts as it works, detecting patterns that are normal for specific customers, and abnormal for others. Housed in a centralized Enterprise Case Manager, investigators have only one place to go for relevant information for each case.
Web fraud poses a major threat to your institution.

Whether it’s with advanced Trojan techniques for inserting malware into corporate computers or “man in the browser” technology that penetrates browsers, hackers hijack user credentials and change the data sent to the server.

Your reputation is on the line.

Customers expect their data to be protected, and inadequate risk management can leave your company at risk of losing both money and customers.

More than $781 million was reported lost due to web fraud in 2013.

FBI, IC3 Report 2013

- Create detailed behavior profiles for online application users.
- Respond to changes in “normal behavior” across a wide range of scenarios.
- Reduce identity theft, account takeover, man-in-the-browser, and DDOS attacks.
How it Works:

As customers interact with the online application, a profile is generated. This profile identifies and stores patterns, creating a complete picture of a particular customer’s typical activity. If a customer interacts in ways that veer away from their stored patterns or rules, an alert is created and their account can be suspended and investigated.

Examples of Rules:

**Rule:** Sign-in attempts
**Alert:** A customer attempts to sign in from a different and suspicious geographical location in a given timeframe.
A customer attempts to sign in using a different fingerprint within a short period of time.

**Rule:** Outbound transactions
**Alert:** A new or reactivated account performs multiple outbound transactions of a large amount.
A customer attempts an outbound transaction that has been marked as high risk.

**Rule:** Payments to new payees
**Alert:** A customer attempts an outbound transaction to multiple new payees within a short period of time.
The stakes are high.

Noncompliance fines can cost millions of dollars. Antiquated sanctions screening solutions don’t provide the compliance you need to stay compliant with anti-money-laundering laws.

Protect your financial institution with compliance, all in one place.

With Bottomline Sanctions Screening, each transaction can be checked against any number of sanction lists, including whitelists, blacklists, and customer-provided lists, consolidating your control of both compliance and fraud.
Spotting violations is a two-step process.

After first ensuring that your sanctions list data is refreshed, you must commission and manage the infrastructure to screen day-to-day transactions in real time. These two steps alone are time-consuming, and violation investigations take infinitely more resources.

False positives put a strain on your scarce resources.

Your time shouldn’t be spent investigating false positives. With little margin for error and deadlines to meet, traditional solutions make saving time and money a serious challenge when every potential violation is flagged.

Stay compliant with anti-money laundering laws.

Keep up to date with access to over 100 sanctions lists globally.

See relationships between individuals and groups.
Bottomline Sanctions Screening

How it Works:

As they are screened, red flags are made available in a central dashboard for easy review and rapid action. The investigator is equipped with the match and any other relevant information to perform due diligence to ensure compliance with anti-money laundering laws.

Features Include:

**Transactions Screening:**
Once a payment file is sent, it’s run against your selected sanctions lists.

**Precision Matching:**
You can control the level of precision required for a match to be flagged. 100% will only return exact matches, while lower percentages will return results scaled to the users’ settings.

**“Good Guys” List:**
Upon identification of new false positives, you can move the name into the list to prevent future flags.

By entering a personalized false positives list, you can minimize time wasted investigating false positives.

**Intelligent Word Matching:**
In order to match transactions to the various fields in transaction lists, Sanctions Screening uses an optimized Levenshtein distance algorithm.

**Duplicate Checking:**
While checking against various sanction lists, Sanctions Screening can also flag any duplicate transactions that contain the same information based on key data in the transactions.

**List Management:**
While this solution maintains preconfigured lists, you can add your own black and white lists. These lists are updated constantly to ensure the latest sanctions information is available.
An international long-term savings and investment group, with more than 12 million customers and 55,000 employees worldwide, implemented Bottomline Cyber Fraud and Risk Management to help guard against insider fraud. Only five months later, the system had prevented an estimated $2 million in losses from an internal crime ring that had intended to steal company funds. That doesn’t take into account the cost associated with the negative impact on their reputation that would have occurred.
Traditional solutions may collect vital data from log files and provide general database analysis, but it’s not enough. Log files are time-consuming to analyze and they don’t provide the level of insight into all user actions, queries, screen views, and transactions that are necessary to proactively track down and stop fraudulent behavior.

The platform’s data capture and collection approach is comprehensive. All data exchanged on the monitored applications across a corporate network is recorded via patented network-sniffing technology and available for viewing and investigation in real time. The solution can capture data from text and binary files, log files, database tables, XML and CSV files, user queries, message queues, and other sources.

Encrypted using 128/256 AES, and digitally signed with MD5 and RSA, the recorded data may be acceptable as forensic evidence in the U.S. court of law.
Dynamic profiling allows the system to learn and adapt, helping to define what activity is normal and what is suspicious.

The challenges posed by profile and alerting involve effectively developing behavior analysis that can identify suspicious behavior—while keeping false positive rates low. Traditional solutions cannot alert on targeted behavioral scenarios and tend to generate more alerts than a company can handle. The platform gets smarter over time, providing better visibility, generating less false flags, and more true potential instances of fraud—resulting in more accurate alerts for your team.

The platform’s data model can maintain static and dynamic data on employees, accounts, and customers. As the system profiles each user or user group, the data is relayed with full transparency to the discerning analytic engine.

The analytics engine applies a risk score to unusual actors, generates immediate alerts, and limits the rate of false positives. The rules and scoring functions can be tweaked and fine-tuned to ensure its continued success.
Due to complexity, system and department silos, limited log capturing, and an overwhelming number of false positives, investigations are difficult to manage.

The Investigation Center is the hub where you can perform all activities in the investigation lifecycle. It is composed of a set of integrated functions, each assisting the investigators with various facets of fraud investigation and resolution.

**Alert and Case Manager:**
Assists investigators in the prioritization and review of captured suspicious activity from beginning to end.

**Unique Replay Capabilities:**
Allows investigators to re-watch screens where suspicious activity occurred (even if screens were merely viewed), giving full context into the actions performed.

**Cross-Platform Search of User Activity:**
Perform a Google-like search on the content of all screens accessed by users across disparate systems in a given timeline to find, for example, all users who accessed a specific customer account in a specific timeframe.

**Link Analysis:**
Visually display relationships between employees, customers, accounts, and many other parties. Fraudulent entities, or those under investigation, are highlighted to allow further examination.

**Control Business Rules:**
Allows investigators to manage the scoring function to reduce false positive rates.
About Bottomline

Is your privacy and data security solution able to stand up to the evolving threat landscape? Find out how you can stay ahead with this informative video.

To learn more about Cyber Fraud and Risk Management solutions, visit Bottomline Technologies at www.bottomline.com or contact:

Phone: 800-472-1321
Email: info@bottomline.com

About Bottomline Technologies
Bottomline Technologies (NASDAQ: EPAY) powers mission-critical business transactions. We help our customers optimize financially-oriented operations and build deeper customer and partner relationships by providing a trusted and easy-to-use set of cloud-based digital banking, fraud prevention, payment, financial document, insurance, and healthcare solutions. Over 10,000 corporations, financial institutions, and banks benefit from Bottomline solutions. Headquartered in the United States, Bottomline also maintains offices in Europe and Asia-Pacific.