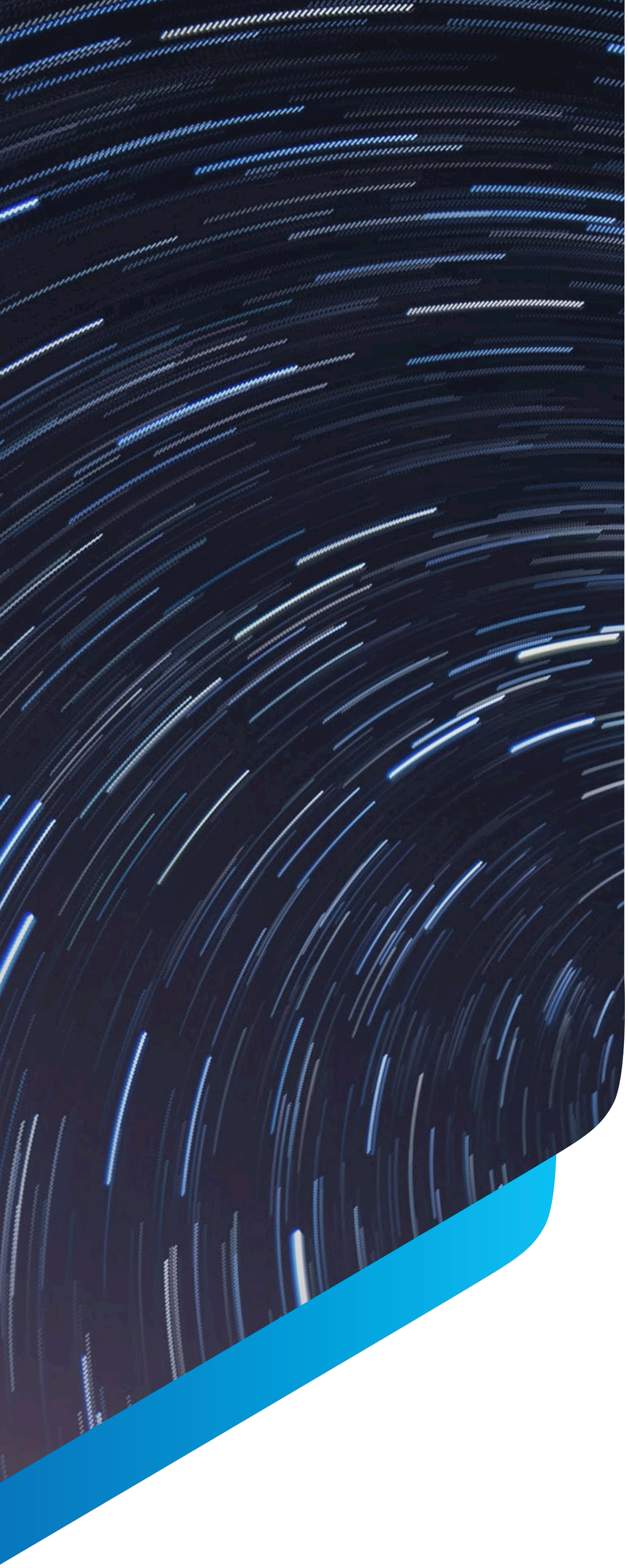
Bottomline



Fight Fraud and Financial Crime with a 360 Degree View

As Cybercrime Converges, Fragmented Views of FinCrime Fall Short

For criminals looking to cash in, opportunities to commit fraud and other financial crimes have never been so plentiful. Advances in payment technology, such as transaction options like Venmo, WorldPay and AliPay such as those from Apple and Qiwi, always open doors to new risks. The recent rise of cryptocurrency is also presenting new challenges. And in the past 12-18 months, the increase in remote work and transactions has put pressure on even the best-prepared institutions. As Julie Conroy of Aite explains, “The COVID-19 pandemic has starkly defined financial, social, and even financial crime trends throughout 2020 . . . few were prepared for the gigantic wallop that the year had in store.”[1]

Unfortunately, most financial institutions’ case management tools across their enterprise have not kept pace with the rate of change. In fact, according to a recent McKinsey report, it is estimated that $800 billion to $2 trillion in proscribed transactions is moved through the global institutional system annually —yet authorities intercept less than 1% of those amounts.[2] Investigators are trying to fight sophisticated criminals with technology that is the equivalent of having one hand behind their back, while financial institutions are trying to satisfy their customers and protect their business interests with tools that are not fully up to those tasks, either.

The key to this struggle lies in the segmented structure of the teams and tools that financial institutions have in place to fight criminal activity. While different types of financial crimes have begun to converge, most organizations still have their analysts addressing specific crimes instead of specific customers without a consolidated view across the FI.

The Fallout of Fragmentation

When different teams in different places are looking at different data, they lack a holistic view and face several challenges that complicate the task—and costs—of fraud detection, crime investigation and regulatory compliance. These include:

SILOS

Hidden risk is the most dangerous kind because you can't address what you can't see. When investigators and analysts work with only a partial picture, they can miss important red flags.

OPERATIONAL REDUNDANCY

A byproduct of silos is the inadvertent duplication of people, tasks or tools. Not only can it cause confusion, such inefficiency is also a wasteful expense.

CUSTOMER SERVICE VS SECURITY

Financial institutions must balance the need to catch criminal activity with the need to provide good customer service. Under pressure in the real-time payment environment, too many alerts or false positives can result in them being ignored or customers complaining about friction in the transaction process.

CUSTOMER COMMUNICATIONS

When it comes to tracking the progress of disputes, customers expect timely, accurate information—which is not always possible if their bank is operating in silos.

COMPLICATED COMPLIANCE

As financial technology and crimes increase in complexity, so do the regulations that govern them. A fragmented view of customer activity can lead to missed violations and costly fines.

In short, failure to overcome these challenges can leave financial institutions struggling with financial losses, the cost of compliance and regulatory pressure, as well as customer friction.

So what does a better way look like?

ENABLE YOUR INVESTIGATORS WITH A 360 DEGREE VIEW

Bringing together fraud and financial crimes, known as FRAML (fraud and anti-money laundering) under a single purview can help close the gaps. With a fragmented approach, it takes too long to find accurate, updated information and put it all together. But a 360-degree customer view that consolidates risk can vastly improve both investigations and calculations. Connecting the dots with an all-encompassing view tells a visual story that makes it easy to spot issues and deal with them before they become a problem.

What are the main challenges you face during the investigation process?

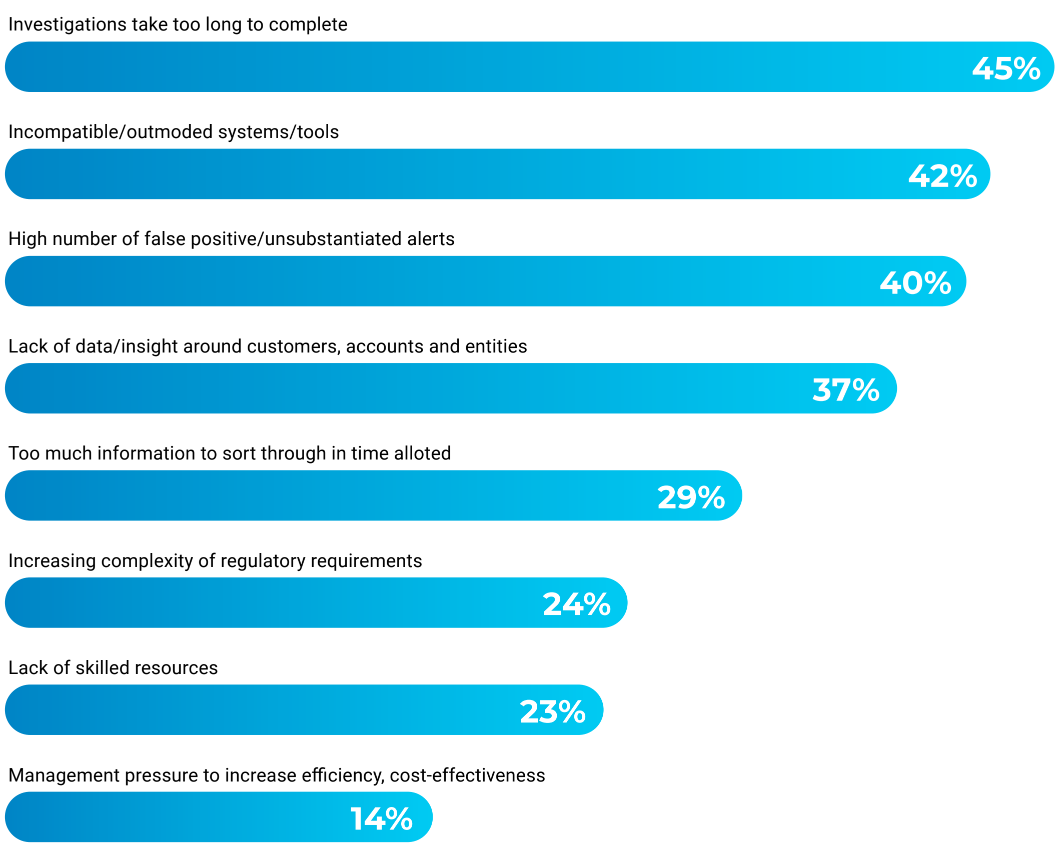


Figure 1: Risk.net Survey Report “Smarter thinking around financial crime prevention”. January 2019

Add Business Value

It's important to remember that proper case management encompasses more than just unifying investigators who fight fraud and other financial crimes. Direct loss from criminal activity is only one element—a very big one—but there are two key areas of concern that can affect a financial institution's profitability.

First is the ability to avoid exposure to financial penalties by understanding how much risk a particular customer may pose in terms of not only fraud, but money laundering and sanction embargoes.

Second is the issue of cost control. It is extremely expensive to find the skilled personnel in the financial crime space in general and get them up to speed. These are highly experienced, highly compensated individuals who are in scarce supply. It is critically important to introduce automation into the equation when possible to reduce the need for hard-to-find personnel.

There are tools that make it possible to reduce exposure and contain costs, but it takes careful evaluation. Some of the key criteria to look for in a solution include:

1 **ACCURACY:** The quality of alerts is a key issue—FIs want to minimize false positives as much as possible, but don't want to overlook risky transactions. This requires using powerful data analytics. Too often, people blame an analytics tool for disappointing results when in reality it is the quality of the data coming into the system. Better quality data equals better quality analytics, period. A good system will be able to enrich data by consolidating it from across multiple sources. In addition, the ability for users to give more input that tunes the system will create alerts that continuously become that much more accurate.

2 **EFFICIENCY:** Reducing silos is one way to promote efficiency and so are optimized workflows. However, automation also plays a key role. On the compliance side, using Robotic Process Automation (RPA) for repetitive tasks such as producing SAR reports means faster completion of required paperwork with less chance for human error. Customer service is another area where intelligent automation—which leverages RPA in conjunction with AI—shines. The ability to automatically raise a dispute, populate it with the right information and keep customers informed throughout the process can increase customer satisfaction while reducing the number of employees needed and the speed of resolution. An additional efficiency feature to be considered is seamless integration with other tools, and the ability to configure a system without needing to code.

3 **INSIGHTFULNESS:** The best tools not only improve fraud detection and prevention, but also business results. A full picture of customers can help FIs monitor financial health as well as conduct financial impact analysis. This enables smart business planning by revealing which customers are truly risky. Even if they don't reach the threshold of requiring a report to authorities, their fraud to transaction ratio may be a trigger to end the relationship.

Of course, not all threats come from the outside. A truly complete tool will act like a Digital CCTV allowing you to record and replay users action on different applications and systems to monitor internal fraud risks as well.

(The) Bottomline

There has never been a more necessary time for FIs to reevaluate their approach to FinCrime.

According to analysts at the Aite Group, global lockdowns significantly altered the way consumers and businesses transact—and the way organized crime rings operate.[4] This has been enabled by the ever-increasing technological savvy that fraudsters and money launderers have developed to exploit the growing criminal opportunities that new technology provides.

Perhaps that's why, according to Aite Group Fraud and Financial Research Director Julie Conroy, 45% of North American institutions are focused on converging technology.[3] However, that move is not something that most organizations can successfully accomplish on their own. When it comes to selecting a partner in your shift to a single-pane view, depth of knowledge and experience with financial fraud is crucial. Bottomline has been at the forefront of business payments and fraud prevention since 1989. As a market leader in fraud detection, 90% of top US banks trust Bottomline solutions, as do 5,300 corporate customers across 92 countries. For an Enterprise Case Management solution that is complete, comprehensive and efficient, join these companies in trusting Bottomline.

> "If you do not have a holistic view of what is going on, there are likely some areas of risks that you do not see. And that's what is needed—to identify the areas of where the risks are in order to take action to eliminate those kinds of risks."

FOOTNOTES

1,3 https://www.aitegroup.com/report/top-10-trends-fraud-aml-2021-onward-and-upward

2 https://www.mckinsey.com/business-functions/risk/our-insights/the-investigator-centered-approach-to-financial-crime-doing-what-matters

Bottomline

Connect with us

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**

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
ap_info@bottomline.com