Bottomline

If You Can't Secure Your Payments,
You Won't Secure Your Commercial Customers:

Why Every Bank Needs a Proven Fraud Protection Solution

As consumers are exposed to more sophisticated technology in their personal lives and interactions, innovation becomes the standard by which they evaluate all aspects of their lives, including business interactions. Tech giants such as Amazon, Google, and PayPal all reinforce the immediate gratification of next day shipping, information at your fingertips, and instant fund transfers…it's no surprise that consumers increasingly demand the same types of products and services from the organizations with which they do business – including their commercial banking partners.

In response, financial institutions have been undergoing a 'digital transformation' as the industry scrambles to meet customer desire for flexible online account opening options, faster payment capability, and access to services from the mobile device of their choice.

And if meeting those needs didn't add enough pressure to banks fighting to remain competitive, the very nature of those technological innovations comes with its own host of problems including increased exposure to cyber-criminals who are waiting in the wings to exploit those digital channels.

No payment method is safe from cyber-crime attack. Checks (74%), ACH transactions – both off and online (55%), wire transfers (40%), and commercial credit cards (34%) are all targets of cyber-criminals and the number of attacks is rising year after year. In fact, 30% of organizations reported an increase in experienced fraud attacks in 2019.[1]

Why is cyber-crime so rampant and why are cyber-criminals able to conduct successful attacks on even the most recent payment schemes? The answer lies in the shift of cyber-criminals banding together to act like businesses, enabling them to escalate financial fraud into 'cyber-crime as a service'. Just as digital technology allows banks and financial institutions to provide customers faster transactions across multiple platforms, including mobile devices, it also allows criminals to deploy multiple attacks to multiple targets with just a push of a button. Business Email Compromise (BEC) is a perfect example of a tactic cyber-criminals use to send blasts of false emails directing employees to misdirect funds or change banking account information. Even with a low success rate, multi-pronged attacks like these are still lucrative for criminals.

BOTTOMLINE SECURE PAYMENTS

- Out-of-box solution for lower total cost of ownership
- Published API provides seamless payment hub integration
- Consolidation of multiple fraud solutions

It may seem like it's all bad news when it comes to fighting financial crime. But there are ways to protect your organization against BEC and other types of cyber-attacks while preventing the diversion of funds into the accounts of bad actors. In fact, according to the 2020 Treasury Fraud and Controls Survey, organizations with payment fraud detection solutions in place that incorporate interdiction technologies see 75% fewer losses in certain types of fraud.

The importance and effectiveness of a payments fraud prevention solution is further illustrated by the following real-world examples of customers who trusted Bottomline Secure Payments to protect their financial institutions and customers from cyber-criminal attacks.

Although these featured banks had very different profiles, the requirements for a fraud prevention solution were the same:

- Proactively detect and prevent payment fraud attacks
- Employ rules-based detection and behavioral profiling
- Generate real-time alerts for suspicious events

CUSTOMER PROFILE

- Community bank
- 25+ years in business
- 150 branches

COMMUNITY BANK CUSTOMER SUCCESS STORY

In the ongoing fight against fraud, an award-winning community bank regularly evaluates its fraud prevention measures to ensure it has the strongest defenses in place to protect customers and their funds from multi-faceted cyber-attacks.

This community bank partnered with Bottomline to digitally transform their product and services offerings and simultaneously ensure the latest fraud prevention measures are deployed to deter cyber-criminals.

The digital transformation journey began with the bank adopting Bottomline's Digital Banking IQ™, a customer-centric digital banking and payments cloud solution that provides cash management capabilities, allows for payments innovation, and enhances customer relationships with rich insights derived from data analytics. The out-of-the-box solution includes Secure Payments, Bottomline's cyber fraud and risk management enterprise solution for financial institutions.

The bank understands the importance of risk scoring payments, so Bottomline worked with the bank and its e-banking software provider, to make the integration with seamless with the ability to risk score Fedwire payments that are processed through the bank's 3rd party Payment Hub. The bank also needed the ability to risk score and identify anomalies in ACH files that are processed independent of the e-banking solution ("offline" ACH).

One major advantage of Digital Banking IQ and Secure Payments, is that they are designed to work together out-of-the-box and do not require any integration effort, customization or tailoring. This minimizes the effort and time to get to going live and of course makes Secure Payments a very cost-effective solution. Instead of installing and deploying, the solution can be activated and onboarded which lowers the total cost of ownership. The bank enjoyed another major advantage of Secure Payments: its ability to risk score based on a "bigger picture" of payments arriving from multiple additional online and offline channels, this robust capability helps detect sophisticated fraud schemes that span multiple channels.

The solution also provides a consolidated view of alerts in the proprietary 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 with flexible drilldown options on each related entity. And with the Secure Payments hosted in Bottomline's cloud, the bank has peace of mind that any security updates and enhancements would be taken care of automatically.

GLOBAL COMMERCIAL BANK CUSTOMER SUCCESS STORY

In this second example, the customer is a global commercial bank with a banking network that spans 6 continents. In addition to the objectives above, the bank was also looking to consolidate disparate fraud solutions into one enterprise fraud management solution. This consolidation would give the bank a holistic view of all payments activity across all locations – equating to an exceptionally high volume of daily transactions, more than 1 million. This would allow for a more accurate and efficient risk scoring process to detect and block anomalous activity before funds could be diverted.

Like the community bank previously referenced, this global commercial bank chose Bottomline for its online banking needs, and added Secure Payments to protect its multiple channels (ACH, Bacs, Wires, check and more) in the US and across the globe. Unlike the community bank, this financial institution started with hosting Bottomline's Secure Payments on its on premise, private cloud and is now planning the transition of the solution to the Bottomline cloud.

At every phase of the project, Bottomline and the bank held design sessions to clarify the bank's objectives and tailor the solution and recommend added services as necessary to meet those objectives. Once the scope of the project was outlined, the deployment of features was prioritized to maximize value and efficiency. Training was also provided to empower the end user teams to be self-sufficient once the solution was live. Bottomline and the FI designed the phases in a way that constantly added business value with minimal risk.

With Secure Payments in place, the bank is monitoring the majority of payment activity and transactions throughout the enterprise. The behavior of customers, employees and other users is tracked and profiled by the analytics engine which correlates the activities between Bacs, Wire and payments. When suspicious activity is detected, real-time alerts are generated and displayed in the Investigation Center, which provides a centralized dashboard for ease of review by its Fraud Investigative Unit.

CUSTOMER PROFILE

- Global commercial bank
- 35+ years in business
- Located in 7 countries

NEW CONFIDENCE

Both banks continue to expand the use of Secure Payments, adding new payment types and protecting a growing number of funds across the financial institutions and mitigating the risk of lost or misdirected funds. And the ability of Secure Payments to monitor payments coming in from multiple channels, the banks have a more holistic view of payments overall and subsequently able to detect even the most sophisticated fraud schemes.

Whether your financial institution is a community bank or a global commercial bank, Bottomline's Secure Payments can be scaled to provide you with real-time payment fraud protection and continuous risk assessment. Leveraging the latest machine learning technology, rich reporting visualization and sophisticated forensic tools, Secure Payments reduces your bank's risk profile and increases the effectiveness of your investigators.

Learn how your organization can protect multiple payment types across a variety of application and channels before fraud occurs, rather than after the damage is done.

DOWNLOAD NOW

1. 2020 AFP Payments Fraud and Control Report

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