Bottomline
FRAUD AND FINANCIAL CRIME SOLUTIONS

Authorized and unauthorized fraud in the era of payments innovation

Get wise to the threat

It's a constant challenge for banks and businesses to keep up with the fast-moving payments landscape as many are faced with a multi-faceted tsunami: constantly evolving technology and ever-present competition, growing fraud typologies and scams, limited resources, ever-tighter regulatory and political pressures, while maintaining a near frictionless customer experience.

Now, they have the added burden of surviving the effects of a global pandemic. With everyone forced to become more digital, connected and ubiquitous (anytime, anywhere, from any device), the world of payments is also becoming faster and more distributed. Over the last decade, an increasingly digitally savvy population, challenging economic conditions and technology advances have made new life models possible (e.g. through the gig economy) and faster and simpler interactions a necessity. At the same time, fraudsters have access to the same technological advancements. This more casual, conversational and immediate nature of digital payments, already well established in B2C payments, is now also pervading the B2B payments world[1&2].

As organizations are forced to evolve their working practices and technical infrastructure faster than they would normally have done, they also have to contend with the need to process ever richer data, as driven by modern payments standards such as ISO 20022. We know fraudsters thrive in fast changing environments. Therefore, if payments are becoming so much faster, easier, more frequent and data-rich, aren't they also even more conducive to crime and fraud than they were before?

The business challenges of an evolving fraud landscape

Financial crime is one of the largest systemic risks to the global economy and associated costs are estimated to be between £1.4 trillion and £3.5 trillion[3].

Organized crime set-ups mirror some of the most mature corporations, with knowledge sharing and cooperation, technology innovation, services, and tools that optimize fraud operations across geographical boundaries. And perhaps their biggest advantage is that they are unhampered by any regulatory obligations.

By contrast, organizations are faced with the challenge of having to protect not only their own environments, but people's personal data everywhere, and having to tackle fraud and financial crime wherever it happens. Driven by consumer expectations and faced with increased regulatory pressures, they also have to do it in near real-time, without hampering the user experience. Governments are faced with the same challenges, as they try to develop regulations that encompass new technologies, but also combat new crimes, all the while attempting to foster innovation and competition.

In this cat and mouse game, banks and businesses have to resolve the conundrum of having to handle ever richer data while facing the associated increase in responsibility and accountability. Financial services organizations have long been used to tackling this issue by the very nature of their business, but even they are finding it hard to face the onslaught and their resources are under pressure.

Existing fraud prevention processes, such as manual reviews, are often no longer fit for purpose because of the increasingly immediate nature of financial transactions, which now require quasi-immediate intervention. Corporations in other industries, not as heavily regulated or resourced and having to process just as much data, find it even more difficult to tackle this challenge. For all businesses, investigator time to resolve an alert has become a key performance indicator. Some may tighten fraud thresholds (e.g. limit cross-border transactions, types of goods, or amounts) to resolve the issue, invariably leading to revenue loss as a result of false positives.

In addition, with payments innovation spurring the increase in digital and mobile payment activity during the pandemic, new threats are emerging all the time and businesses suffer from the lack of knowledge of available and trusted third-party data to assess the threat landscape and distinguish genuine from fraudulent interactions.

As digital payment activity increases, so too does the amount of data generated, providing more opportunities for criminals to steal sensitive business and personal information for the purposes of fraud. Therefore, the lack of visibility or tools to derive actionable insights, as well as the limited amount of cooperation within and across industries and geographies, makes tackling both authorized and unauthorized fraud, internal or external, one of the top concerns of businesses today.

The US Federal Reserve FraudClassifier model[4] aims to classify fraud independently of payment type, channel or other characteristics. Whilst not used in other geographies, it offers a helpful classification model:

WHO INIATIATED THE PAYMENT?

Authorized Party **How was the fraud executed?**	**Authorized Party** Was manipluated	***Q: How was the Authorized party manipulated?***	Product & services fraud or
			Relationship & trust fraud
	Authorized Party Acted fraudulently	***Q: How did the Authorized party act fraudulently?***	Embesslement or
			False claim or
			Synthetic ID
	Authorized Party Modified payment information	***Q: How did the Authorized party modify the payment information?***	Compromised credentials or
			Impersonated authorized party or
			Physical alteration
Unauthorized Party **How was the fraud executed?**	**Unauthorized Party** Took over account	***Q: How was the Unauthorized party take over the account?***	Compromised credentials or
			Impersonated authorized party
	Unauthorized Party Misused account information / payment instrument	***Q: How was the account information / payment instrument misused?***	Digital payment or
			Physical forgery / counterfeit

01

AUTHORIZED FRAUD

Authorized fraud, by its very nature, is difficult to detect, because the party performing the transaction has legitimate authorisation to do so.

The most commonly understood type is **first party fraud**, which occurs when legitimate account holders misrepresent themselves to obtain products or services (e.g. obtaining more favorable credit rates or insurance premiums, false insurance claims, chargeback fraud). Where first party fraud involves legitimate users intentionally committing fraud, legitimate users can also be led to initiate unintentional fraud, such as **Authorized Push Payment** fraud (APP). This usually start with a phishing or spear phishing attack where fraudsters target people with financial responsibility (e.g. operating a bank account), and involves compromising an email conversation to lead someone into making a payment to an account operated by a fraudster. This step is generally referred to as **Business Email Compromise** (BEC)[5] and sometimes as CEO fraud. The global increase in digitization and instant payments has led to a comparable increase in this type of fraud[6&7,] and money transferred generally disappears very quickly.

Whilst APP fraud - involving legitimate users in a position of responsibility - is unintentional, we also observe a rise in intentional fraud committed by this type of user, and **internal fraud** (e.g. procurement or invoicing) is a well-known challenge in B2B payments[8].

The operation of **mule accounts** is another commonly understood type of fraud involving legitimate users. This occurs where genuine account holders are either convinced or coerced into allowing third-party funds to pass through their accounts, generally on the promise that they can keep a portion of the funds as a reward for their help. In most cases, mule account holders are not aware they are committing fraud or that the funds they handle are either the proceeds of crime, or intended to facilitate crime.

The fraud types described above involve genuine account holders, and all are difficult to detect. This is because the challenge involves trying to determine the **intent** of the interaction (e.g. did they mean to do it?). Whether the intent is malicious, or uninformed, or simply trying to fulfil an obligation during the normal course of work, recognising the interaction for what it is also requires visibility and understanding of **circumstantial behaviors** (e.g. is the user under pressure? Is this usual behavior?). To add to the pain, the current pandemic has exacerbated the upward trend for authorized fraud[11] as criminals always find ways to capitalize on major events.

Insights

Since the pandemic pushed more transactions online, scammers have been busier than ever: the volume of BEC attacks increased by 15% during Q3 2020, affecting more than 75% of industries tracked[9].

In the first half of 2020, UK Finance reported £207.8 million in fraud losses due to APP fraud, representing a 15% increase over the previous period[10].

The average cost of insider threats is rising, with a 31% increase from $8.76 million in 2018 to $11.45 million in 2020[11].

02

UNAUTHORIZED FRAUD

Unfortunately, not only do businesses have to find ways to combat authorized fraud, criminals are becoming more and more innovative in committing fraud of a different nature: unauthorized fraud.

The sadly all too frequent data breaches which have become part of life continue to give criminals many opportunities to monetize stolen identity credentials as billions get dumped on the dark web often at very little cost – credentials and sensitive personal details can be obtained on criminal forums for as little as $12[13]. Indeed, unauthorized fraud is intrinsically linked to **identity theft**.

Fraudsters can use stolen credentials to create new accounts, and this often remains unnoticed by the genuine account holder, until they themselves decide to apply for a financial product and discover, for example, that their credit rating is very low. **New account creation** fraud is relatively simple to execute, extremely common, and can easily be automated. An emerging, and less understood, variant of new account creation is **synthetic identity fraud**. This is similar in intent and outcomes to first party fraud, the only difference being that the identity presented, whilst appearing to have the attributes of a genuine identity, is fictitious. Synthetic identity fraud is perpetrated by combining fictitious data (e.g. name, driver's license and address) and sometimes genuine information (e.g. a real government or other trusted identifier, often from a child, the elderly or homeless) to create brand new identities to commit fraud. Generally, these fake identities lay dormant for months, sometimes years, until they establish enough financial history (e.g. small purchases promptly paid), and the opportunity for "bust-out" presents itself (e.g. applying for a large loan, with no intention of repaying it).

Fraudsters can also use stolen credentials to take over existing accounts, referred to as **account takeover fraud**. This also can be easily automated, driven not only by the sheer volume of stolen credentials available on criminal forums, but also by the persistent practice of password sharing amongst users at large. Indeed, many reputable brands have been the subject of highly publicized **credentials stuffing** attacks. A variant of account takeover fraud can also be observed in the corporate context, where criminals socially engineer individuals in positions of authority (usually through phishing or spear phishing) for the sole purpose of gaining access to the corporate environment. Of course, once a privileged account is compromised, the potential damage to an organization can be extraordinary.

As technology advances, it becomes clear that traditional methods and processes (e.g. rule-based, passwords) are no longer sufficient to tackle modern financial crime.

What does success look like?
From hindsight to insight...

The fraud types mentioned here all have one thing in common. They all rely on compromising identities in some fashion.

As digital identity has become an intrinsic and growing part of financial services, and of the payments industry in particular, increased digitization leads to opportunities for businesses as they launch new products and services, perhaps a bit faster than they would normally have done. To do all this of course requires more and more data, which is becoming even richer and more useful thanks to modern payment messaging standards such as **ISO 20022**. As mentioned, this leads to an even more conducive playground for criminals, who will very rapidly find weaknesses to exploit in new services and products. **Richer data** comes with greater risk and responsibility.

In order to compete in this fast-moving world, and as customers adopt new services and new threats emerge, organizations should:

- **Ensure that they deploy dynamic approaches to fraud prevention, balancing smooth experiences with security.** Solely relying on passwords, on even multi-factor authentication will not solve the multi-faceted problem of modern payment fraud, and manual reviews, or any labor-intensive tasks, must be kept to a minimum.
- **Be able to recognize legitimate customers across industries, channels and geographies, fast**. This will enable them to counter the proliferation of stolen identity credentials and advanced device and identity spoofing techniques which allow fraudsters to bypass the most complex screening procedures.
- **Use automation in order to intelligently sift through the vast amounts of data generated in the payment ecosystem and ensure that it is of good quality.** This will enable them to manage the added increase in regulatory pressures, the limited resources available and a challenging economic climate.
- **Be capable of understanding context** (e.g. Which device? Where? At what time?) and other relevant attributes (e.g. Do they normally behave in this way?) as well as supplement what is traditionally known about a payment interaction to derive actionable insights. This suggests the adoption of technologies, such as **machine learning**, to identify patterns and other relevant attributes not generally uncovered by other methods. For example, determining whether a consumer actually intends to make a payment is not generally uncovered by traditional methods, as exemplified by the rise in authorized push payment fraud.

What does success look like?
From hindsight to insight... *(Continued)*

Solving this conundrum can be a challenge and some businesses struggle to deploy technology environments enabling them to capitalize on data. Complex integrations with existing systems can also often result in deployments taking many months, if not years. Furthermore, ensuring that chosen solutions are based on modern and open technology stacks is key to future proofing infrastructure.

Fraud knows no boundaries, so businesses must also keep constant watch on the threat landscape. This means having access to reputable cross-industry and cross-geography data sources so as to enrich and inform their prediction models to make derived insights as relevant as they can be.

But automation, and technology, alone cannot solve this problem: insights can only be actioned effectively if relevant **processes** are in place and **people** are able to adapt to modern practices. Then and only then would they be able to move from hindsight to insight, and effectively combat fraud in an increasingly digital world.

Why Bottomline?

We are at the forefront of making complex business payments simple, smart and secure. Thousands of banks and corporations worldwide rely on us not only for domestic and international payments, efficient cash management, automated workflows for payment processing, but also for state-of-the-art fraud detection, behavioral analytics and regulatory compliance solutions.

Not only do we understand payments, we are focused on providing easy-to-integrate services through our cloud-based infrastructure and APIs. Taking advantage of our innovative solutions never means months or years of integration: businesses are up and ready to capitalize on insights within weeks.

Because we also manage payments, we're in a unique position to be able to capture and analyze raw traffic data to derive actionable insights. We provide bank-grade analytics to all our clients, easily.

We can make businesses more efficient as we also understand that manual reviews, whilst sometimes necessary, should be kept to a minimum. We also understand that false positives are bad for business.

A large bank in Central Europe who implemented our Secure Payments solution was able to stop a sizable fraudulent transaction within the first seven hours of going live.

Between November 2018 and November 2020 Bottomline processed over $500 billion in payments:

- Zero fraudulent payments were made over our payment network.
- We blocked over 250 attempts to intercept high value payments, including tactics such as vendor account takeover and business imposters.

Why Bottomline? *(Continued)*

Our Fraud and Financial Crime Management solution suite enables banks and businesses to succeed in their challenging journey towards modern and secure digital payments. We help our clients reduce risk, protect against financial crime and simplify their regulatory compliance obligations through a set of innovative solutions:

- **Secure Payments:** This multi-layered security solution consists of four pieces of functionality which protect business processes throughout the entire payment lifecycle: Data at Rest Protection, Secure Data Transfer, Intelligent Transaction Monitoring and Segregation of Duty. An additional optional module, Security Without Intervention, offers a cloud security module for customers wanting to streamline digital payments – including ACH, BACS, RTP, Wires, Faster Payments etc.
- **Payee-IQ:** This helps to combat APP fraud and reduces the ways that fraudsters can dupe anyone into sending authorized payments into criminal accounts. Bottomline provides best-in-class beneficiary intelligence, so that corporate clients can have confidence in who they're paying, and so that bank fraud investigators can focus their time on the alerts that are most likely to be fraudulent.
- **Insider and Employee Fraud:** Making use of machine learning and rich analytics, this solution captures real-time user behavior across all critical systems to quickly identify and record anomalous user activity for simple, effective and fast investigations.
- **Enterprise Case Management:** This solution offers an enterprise-wide case management system for creating and managing alerts, suspicious activity cases and report filings. It removes the need for manual collection and processing of data by providing actionable insights to support decision making, reducing investigator time and cost through greater efficiencies.
- **Compliance:** Through advanced analytics including machine learning and behavioral and peer profiling, this solution enables businesses to reduce costs whilst managing the operational and technical burden of rapidly changing financial crime prevention rules and regulations. This solution consists of three features: AML transaction monitoring, Know Your Customer (KYC) and Watchlist Screening.

From hindsight, to insight…to foresight

The new world order in which we find ourselves today has transformed the global landscape for payments. As businesses strive to innovate and deliver the seamless digital experiences that everyone now expects, they must do so in a hyper-connected world and process ever increasing amounts of data. Unfortunately, this creates a perfect storm for criminals targeting the payments industry facing additional regulatory pressures and a growing attack surface.

Successfully managing this transition is certainly possible, but will require strategic focus on:

- Having **end-to-end visibility** of customers, regardless of intreraction, channel or device, and maintaining their trust
- The ability to distinguish between genuine and fraudulent interactions, in real-time or near real-time
- Having access to **trusted data sources and intelligence capabilities**
- Making use of **automation** to reduce manual, data-intensive and repetitive tasks, freeing staff to concentrate on value-adding activities.

Even the most mature organizations struggle to manage continuous change. Deploying a layered approach, through a combination of technology, the right skills, efficient processes, a conducive culture and the right partnerships is the key to success.

At Bottomline, we operate at the heart of the payments ecosystem. With our access to live payments data feeds and extensive intelligence sources, we've built solutions that enable our clients to be successful in this brave new world, moving from hindsight, to insight, to foresight.

We can cut case investigation time by an average of 50% compared to manual reviews.

CONNECT

Learn how Bottomline's Fraud and Financial Crime solutions can provide you with unparalleled protection, while helping you secure your digital channel and comply with regulations.

For more information on how Bottomline can help you, contact us.

Connect with us

About Bottomline Technologies

Bottomline Technologies (NASDAQ: EPAY) helps businesses pay and get paid. Businesses and banks rely on Bottomline for domestic and international payments, effective cash management tools, automated workflows for payment processing and bill review and state-of-the-art fraud detection, behavioral analytics and regulatory compliance. More than 10,000 corporations, financial institutions, and banks benefit from Bottomline solutions. Headquartered in Portsmouth, New Hampshire, we delight our customers through offices across the United States, 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 081 825**0
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

References

[1] https://www.pymnts.com/news/b2b-payments/2020/b2b-payments-crossing-borders-at-digital-speed/

[2] https://www.pymnts.com/news/b2b-payments/2020/bain-capital-ventures-2020-is-b2b-payments-breakout-year/

[3] https://www.ey.com/en_gl/disrupting-financial-crime

[4] https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/

[5] https://www.infosecurity-magazine.com/news/criminals-favor-ransomware-bec/

[6] https://www.finextra.com/newsarticle/35480/app-fraud-losses-hit-456-million-in-2019

[7] https://www.fico.com/blogs/uk-losses-app-scams-are-surging-what-can-banks-do

[8] https://www.paymentssource.com/opinion/the-pandemic-has-awakened-a-hidden-fraud-in-b2b-payments

[9] https://finance.yahoo.com/news/business-email-compromise-bec-attacks-165300765.html?guccounter=1

[10] https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2020-FINAL.pdf

[11] https://threatpost.com/europol-covid-19-vaccine-rollout-fraud-theft/161968/

[12] Ponemon 2020 Cost of Insider Threats Global Report

[13] https://www.helpnetsecurity.com/2020/06/19/dark-web-prices/