Bottomline Technologies

BEST PRACTICES GUIDE

Preventing Fraud in the Payment Process

Facing up to Fraud

If money is the lifeblood of an organisation, it stands to reason that protecting your ability to make and receive payments is vital to ensure your financial heartbeat is free from unnecessary risk.

It is well recorded in the media that fraud is on the rise and closing in, and that fraudsters don't discriminate. Every day businesses of every size and from every sector are hit by fraud, instigated from outside and within the organisation.

Criminologist Donald Cressey theorises that a combination of motivation, opportunity, and justification provides the perfect triangle to commit fraud[1]. Driven by greed or need, you are most at risk where internal controls are weak and existing processes are now inadequate.

Businesses need to now face up to fraud and acknowledge the probability that if you haven't already been a victim of fraud, you are unfortunately likely to be - and those that already have, are likely to be again.

It's time to turn the tables.
It's time to fight fraud.

[1]. *Donald R. Cressey, Other People's Money (Montclair: Patterson Smith, 1973) p. 30.*

Powering and Protecting Your Payments

As a market leader in end-to-end payments and cash management software, Bottomline Technologies can help you safeguard your business payments, reduce the risk and impact of a malicious attack, and ensure business continuity.

Over 80% of respondents admitted to having the know-how and system access to commit fraud in their organisation.

It has been our heritage to ensure that the payable and receivables processes are as efficient as possible enabling enough cash to be available to help you innovate, win and grow. It therefore makes business sense that the technology that powers your payments business also protects it.

Bottomline takes our customers' security very seriously and by naturally extending our payments solutions to provide robust monitoring, validation and security measures your company can proactively manage any suspicious activity within your payment supply chain.

To create the best line of defence we recommend that you take the following steps in process, culture and technology to help decrease the opportunity and ease at which fraud could occur.

1

Step 1: Processes

To pay and get paid without risk is essential, so implementing best practice controls across the business and throughout the payment process is the first step. This, followed by a regular review of potential vulnerabilities, compliance to ethics, rules and regulations, and extending audits and controls is strongly recommended.

In principle, managing fraud risk is the same as managing any other business risk. It's an important element of corporate governance and a key part of the organisation's decision-making process.

CIMA recommends[2] that organisations should:

- Establish a risk management group
- Identify, understand and assess the scale of potential risks
- Develop and implement responses (be that process, education or technology)
- Monitor and regularly review the process

[2]. *Fraud & Risk Management, Chartered Institute of Management Accountants, Feb 2009, p. 20.*

2

Step 2: People

Employees are your first line of defence. Staff members should be well educated in understanding what actions constitute fraud, the negative impact of fraud on the organisation, and ways in which suspicious activity can be reported. ACFE research indicates that organisations that have anti-fraud training programs in place experience lower losses and can detect them more quickly than organisations without such programs.[3]

When a fraudulent activity has to be investigated, it can be disruptive, causing innocent employees to feel defensive and under suspicion unnecessarily. The comprehensive monitoring of user behaviour may seem a little "big brother" but it can help alert organisations to suspicious activity quicker and provide the evidence to identify the actions and employees that need to be targeted for further examination. This leaves innocent employees to get on with their jobs. Technology is the most efficient and effective way of detecting and monitoring irregular behaviour.

Many organisations vet their employees when they first start, usually within a probationary period, including a criminal record check. However, few organisations carry out these checks on a regular basis, meaning the status of long-term employees could have changed. These checks should be carried out annually on all employees, not only on hiring new starters. If staff turnover is high and the automation of processes low, it creates an ideal opportunity for manual intervention and fraudulent activity.

3

Step 3: Technology

A host of technology solutions are available to help organisations detect and prevent the risk of fraud.

Payment threat detection

Examine the actual transaction

- Catch errors and fraud incidents before a payment or collection goes into clearing - for example: validating sort code and bank account details and verifying account ownership upfront ensures you don't pay, or attempt to collect from, the wrong account and incur the estimated £50 cost to rectify it.[4]
- Summary payment reports don't offer transactional detail. Organisations need exception notifications for line by line transaction analysis to highlight suspicious activity against private black lists, warn against duplicate payments, and alert to funds being made to first time accounts.
- Organisations can find it difficult to apply anti-fraud measures upstream because they have multiple systems feeding into a single gateway. So it's important to implement transactional monitoring for every type of payment – payroll, supplier, expenses, and Direct Debit collections to name a few.

[3] *Report to the Nations on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, 2012*

[4] *Bacs, 2013*

Behaviour monitoring

Observe the actions of people

- Committing fraud starts with ‘looking’ rather than ‘acting’. Use technology to alert you to suspicious behaviour. Highlight actions that are out of character and role responsibilities or that contravene processes, controls, regulations and best practice.
- High staff churn is the perfect occasion to process ghost payroll payments. If staff members leave, it’s easy to adjust their records to stay on file and to syphon funds to a new account. Catch duplicate payments to the same bank account.
- Maintain black lists of employee accounts so they don’t appear in supplier or customer payment runs to ensure that payments are only made to valid, correct bank accounts.
- Audits, log files and fraud investigation post fact offers few clues to when, where and how fraud was committed. Conversely, technology offers proactive, real-time notifications when data is viewed or changed. This reduces false positives and investigating irrelevant information. Use graphical tools and screen replays (which are potentially legally admissible in court) to rapidly understand what action was taken.

*It takes **200 days** to detect a fraud and a further **105** to investigate it, so it’s far more beneficial to be alerted to uncharacteristic behaviour early on. Technology also reduces investigation time by up to 90%.*

Security measures

Keep people out

- Manual file upload is not best practice. And moving data between different systems with little automated integration creates the perfect blind spot for file tampering. Use automated, secure point to point solutions to ensure payment files are never at risk and confidential data is safeguarded. Those processing Direct Debits must also consider the refund process and the risk of fraudulent requests.
- The value of Smart Cards has disappeared. They are at risk of being lost, stolen or shared, and accountability is tied to the person owning the Smart Card rather than the perpetrator of fraud. Using a HSM or CSM (hardware/cloud security module) to sign files is more secure, has no physical dependencies, includes audit tracking and offers better control of the approval process.
- Go beyond one layer of verification with multi-factor authentication, to help ensure only authorised personnel are accessing the system. By using a mobile phone device, an additional level of authentication is added to confirm ownership ahead of being able to login and approve payments. Alternatively, bureau solutions also provide the same level of remote yet secure approval functionality.

Face up to Fraud

The technology investment in protecting payments is minimal in comparison to the potential loss suffered due to fraudulent activity. And unfortunately the benefits can never be truly measured until you’re the victim. So if you think your business is safe from fraud, perhaps it's time to reconsider. Have you covered every angle to prevent, detect and respond to fraud and protect yourself from becoming tomorrow's headlines?

At Bottomline Technologies our 20 year history of powering payments for all types and sizes of companies, financial institutions and banks has led us to naturally extend our technology to protect money by keeping it moving in and out of a business securely. As your trusted payment expert and advisor, Bottomline Technologies has the solutions to help your organisation face up to fraud.

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.

Bottomline Technologies®

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
115 Chatham Street
Reading, Berkshire RG1 7JX
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