Transaction monitoring in the digital age
Building on the fundamentals

Transaction monitoring is the practice of tracking the flow of transactions across Information Technology (IT) infrastructure, in addition to detecting, alerting, and correcting unexpected changes in business or technical conditions.

The practice isn’t new – those familiar with correspondent banking and treasury operations are likely to already be aware of a number of screening tools and techniques to mitigate risk from suspicious financial activity. What has changed is the rise of real-time payments, meaning money is now moving and settling faster than ever, so the stakes are higher to intercept any red flags at the start of the payment life cycle. The upshot is that, with the right controls, going to real time can bring corporate treasury in to the 21st century.

The following article is written for corporate treasurers who are implementing faster payment schemes amid a new normal of sophisticated cyber threats, the dark web and the growing acceptance of cryptocurrencies such as Bitcoin.

Acting in real time

The global adoption of faster payment schemes (the engine for mobile wallets) is accelerating a virtual platform where vendors and suppliers expect to settle bills and transfer funds on demand. Currently, 30+ countries are planning to implement, or have implemented, a real-time (or near-real-time) payments system.

In a real-time model, there’s typically a six-second window for a bank to decide if a transaction will be authorised. As a result, as payment systems shift from batch to real-time, there is potential for cybercriminals to commit fraud faster. It’s important to recognise that real-time payments have real-time risk and require real-time screening.

Currently, 30+ countries are planning to implement, or have implemented a real-time (or near-real-time) payments system.

TOR is derived from an acronym for the original software project name, ‘The Onion Router’, and is software that allows users to protect their privacy against a common form of Internet surveillance. On the dark side, websites can’t be found through an indexable search engine; they can only be accessed if you know the web address.

Darknet markets trade illegal products purchased with Bitcoin, and because of the secretive nature of the dark web, it is difficult for law enforcement to eradicate the high risk transactions.

Lurking within the Internet is the dark web, an encrypted network that sits between hidden servers and requires special TOR software to access.

Payment processors, such as money service bureaus (MSBs), face challenges from the dark web. Unbeknownst to them, they may have clients dealing on Bitcoin Exchanges or who are banking (or contemplating banking) Bitcoin Exchanges. They may be unaware that they are moving proceeds of crime associated with Bitcoins that are cashed out on the exchange and could have come from proceeds associated with the TOR marketplace (which includes not only the sale of drugs, but also high grade military weapons, human trafficking, kidnapping etc.).
Know your clients’ clients (KYCC)

With the rise of Bitcoin and the dark web, it is critical that corporate treasurers in general, but treasurers of MSBs in particular, not only know their clients but also their clients’ clients, and perform enhanced due diligence on sources and uses of funds in order to derisk payment operations. Innovative FinTech firms are introducing systems to monitor activity on the dark web and equip financial professionals with analytics to spot and address suspicious activity across digital identities.

It is critical that corporate treasurers in general, but treasurers of MSBs in particular, not only know their clients but also their clients’ clients.

While Bitcoin has a reputation for anonymity, the entire history of Bitcoin transactions is visible to all users, and therefore the blockchain technology/ledger, combined with a monitoring tool, actually allows for increased visibility into potential clients’ activity – more so than would traditionally be available for MSBs.

Currently, the industry establishes a customer profile at onboarding and monitors transactions going forward, verifying that profile. In the Bitcoin space, if you know the addresses of a potential customer (this question should be included in the future state of KYC processes) or if they’ve been identified in an analytical tool, you can see their entire history of Bitcoin activity prior to onboarding, allowing the firm to make a more informed decision. It should also be noted that these tools do not require system integration or data feeds into the firm’s existing transaction monitoring platforms; they are web-based tools that are vendor-supported, similar to WorldCheck and NexisLexis.

Combining IT and human controls

Alongside use of, and reliance on, systems to spot suspicious transactions, it is important that treasury teams are alert to risks. Increasingly, requests to transfer large sums are followed by callback procedures to verify if the request is genuine. Asking questions, probing into unexpected payment requests and acting when something doesn’t sit right makes business sense. With payment requests increasingly coming from a variety of channels, a combination of IT and human controls are essential to disarm today’s cybercriminals. Corporate treasurers are increasingly willing to compromise on rates of straight-through processing in order to safeguard payments that require investigation.

If you see something, say something

Institutionalising a corporate culture that challenges unusual financial activity in the right way is part of a zero tolerance approach to preventing fraud in real time. Given the virtually instantaneous speed at which faster payments are processed, ensuring the integrity of out-going transfers requires a layered approach to data security including:

1. Detection
   Employee education is vital to prevent user devices from becoming infected with malware. Biometrics (fingerprint, voice and finger-vein patterns) is coming to the fore in digital security, replacing traditional PIN devices as a means to digitally sign payments.

2. Protection
   Online banking and fraud monitoring tools are part of behavioural biometric tools to prevent and detect unusual user behaviour. Fraud payment profiling through risk-based profiles help monitor payment traffic to flag unusual activity.

3. Recovery
   Recuperating funds after they have been released is tricky. Financial institutions work together in these cases but it’s rare to recover the full amount on an after-the-fact basis.

Institutionalising a corporate culture that challenges unusual financial activity in the right way is part of a zero tolerance approach to preventing fraud in real time.
Guidelines for effective transaction monitoring

The following are suggested tips for corporate treasurers to manage real-time payment risk as part of a wider operational risk management strategy:

1. **Build a strong framework** – conduct regular independent third-party risk assessments to ensure transaction monitoring and screening controls are current.

2. **Stay up-to-date with transaction monitoring software** – including screening for blockchain, Bitcoin and cyber threats.

3. **Know your clients’ clients** – institute a comprehensive onboarding process for all counterparties and refresh KYC at regular intervals. Employees should be encouraged to ask questions, particularly regarding requests to add new beneficiaries to payment systems, ERP and TMS.

4. **Do the callbacks** if an e-mail or alternate request for a funds transfer doesn’t ‘look right’ – don’t underestimate the importance of a human touch.

5. **Set Key Performance Indicators (KPIs)** around transaction monitoring to drive continuous improvement – analyse metrics and tune decision engines for operational efficiency:
   - % transactions monitored
   - % false positives
   - % actual hits
   - % exceptions resolved within a prescribed service level arrangement
   - % alerts raised in management review meetings for trend analysis.

**Takeaways**

- It is the role of today’s treasury practitioners to embrace the benefits and risks of real-time payments and implement innovative programmes to stay safely on the grid but out of the press.
- By deploying advanced filtering technologies, combined with ongoing education, companies can derisk business and empower employees as a first line of defence to protect their firm’s finances and reputation.
- The digital age is here and, with respect to real-time transaction monitoring, ‘an ounce of prevention is worth a pound of cure’.

barclayscorporate.com

Every attempt has been made to ensure that the information provided is accurate. However, neither Barclays Bank PLC (“Barclays”) nor any of its employees makes any representation or warranty (express or implied) in relation to the accuracy, reliability or completeness of any information or assumptions on which this document may be based and cannot be held responsible for any errors. No liability is accepted by Barclays (or any of its affiliates) for any loss (whether direct or indirect) arising from the use of the information provided.

Barclays is a trading name of Barclays Bank PLC and its subsidiaries. Barclays Bank PLC is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Financial Services Register No. 122702). Registered in England. Registered number is 1026167 with registered office at 1 Churchill Place, London E14 5HP.

September 2016. 04166BD.

**About the author**

Helene Rosenberg
Director, Cash Management, Global Transaction Banking, Barclays US

In her role within Global Transaction Banking, Helene works with corporations, NGOs and non-bank financial institutions on structuring global cash management solutions in Europe and Africa. Her emphasis is on innovation in payments, the digital client experience and developing ‘go to market’ strategies with clients who are entering new markets.

Prior to joining Barclays, Helene worked at SWIFT where she held roles in Global and Key Account Management as well as Consulting Services, where she launched a niche line of advisory services that included best practices when integrating TMS and ERP platforms. Helene has been published in the London Journal of Corporate Treasury Management.

Credits and acknowledgements to Sarah DiStefano, Director, AML Advisory and Compliance Officer, NY and Miami and Chuck Desmond, Head of Barclays North America Operations.