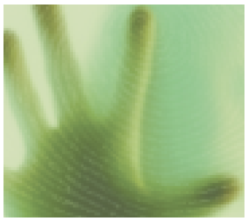
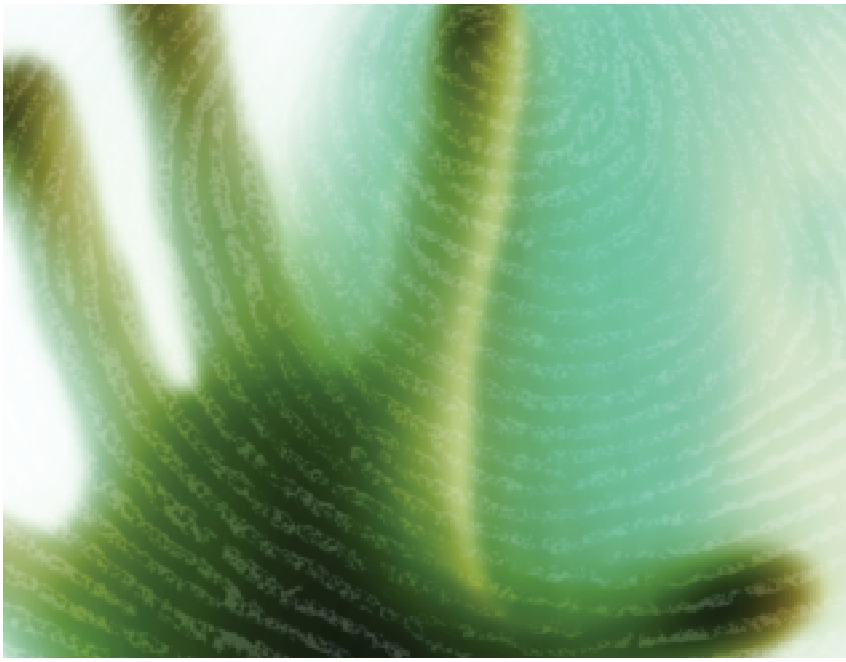




# A question of identity

**JOHN BULLARD** EXAMINES THE ARGUMENT FOR A CENTRALISED PAYMENT FACTORY STRUCTURE AND PROPER EXERCISE OF CONTROLS.




## Executive summary

**While a centralised payment factory solution is fine in theory, care needs to be taken to ensure that the proper controls are in place. Individual identity signing of all actions provides an audit trail. For instance corporates need procedures in place to track who touches the payables file between its release from their Enterprise Resource Planning (ERP) or treasury system and its transmission to the bank. System passwords scribbled on Post It notes and stuck to treasury work stations and multiple employees using a "communal" logon – that never happens in your organisation, right?**


Machiavelli made the following observation about change in 1513: "Leading the introduction of a new order is hard. There is nothing more difficult to take in hand, more perilous to conduct or more uncertain in its success. The innovator has for enemies all those who have done well under the old conditions, and lukewarm defenders in those who may do well under the new. This coolness arises partly from fear of the opponents, who have the laws on their side, and partly from the incredulity of men, who do not readily believe in new things until they have had a long experience of them."

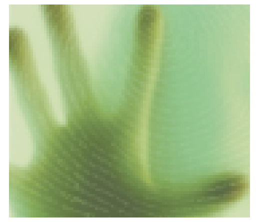
Hundreds of years later, Machiavelli's words are relevant to our current business environment. While companies must continue to evolve and change to gain market advantage and to remain competitive, many fear change and are slow to implement new ways of doing business.

In contrast, marketing-leading corporations recognise the challenges of change and embrace them. Moving to a centralised treasury function – a Payment Factory – is one such change that many are slow to implement even though corporations around the world recognise the benefits that a Payment Factory can bring to their business.

By replacing the current environment of decentralised treasurers and local accounts with Payment Factories, corporations would improve cash management through reducing or even eliminating the need for intra-day integration of accounts across the company. The Payment Factory would also provide internal controls that ensure accountability and auditability. It's critical, however, that the Payment Factory provides accountability down to the individual level.

**THE RISE OF THE PAYMENT FACTORY** The first step in creating a Payment Factory is to transition from a decentralised treasury to a group or centralised treasury operation. To make this organisational change, corporations are leveraging their Enterprise Resource Planning (ERP) software suite or implementing a specialist corporate treasury application. They are developing software interfaces or perhaps purchasing "payment hub" software to handle the many different payment formats. A workflow management system to streamline payment approvals and a rules engine to determine the lowest cost method of payment is also critical. Centralising the treasury function enables corporations to reduce the number of banking relationships they must maintain. It reduces cross-border payment fees and the number of cash transfers by automatically offsetting payments between subsidiaries. This in turn reduces foreign exchange charges, wiring costs and lifting fees from the receiving banks. In addition, the corporation is able to more aggressively negotiate lower banking fees based on higher volumes of transactions with a single bank. Centralising the treasury function also provides corporations with better visibility into funding needs and liquidity management which translates into improved control over payment timing.

**COMPLIANCE AND THE PAYMENT FACTORY** Countries around the world are beginning to follow the lead of the US



regulators and develop and implement appropriate corporate internal controls. The eighth EU Directive includes parallels to the Sarbanes-Oxley (SOX) legislation in the US. France, with LSF (Loi de sécurité financière), Australia, and Japan are legislating rules-based internal controls and countries including China, Canada and South Africa are following suit. Germany has passed a corporate governance code, "a Law for Transparency", from 1998 (KontraG) and a financial directive with SOX-like aspects. Italy's Law 231 and 262, Switzerland's 663 and 728 Swiss Code of Obligation, and the Netherlands Tabaksblad Code incorporate elements of SOX. Other countries such as Hong Kong and the UK are requiring that corporations explain their compliance rather than mandating it; Mexico and Brazil are operating on a voluntary system. Corporate boards of directors are becoming increasingly concerned about liability as a result of news stories of employee fraud, corporate identity theft, computer breaches and malfeasance. As corporations become more knowledgeable about liability risks and the reputational damage that accompanies that liability, they are actively seeking to implement better internal controls and expand and enhance existing tracking mechanisms.

**THE CASE FOR DOUBLE SIGNING** The Payments Factory generates payables that facilitate corporate commerce. While corporations may use different payment forms, these forms are all supported by national or global payments standards. For instance, most originating payments systems require appropriate authentication and authorisation validation before approving and releasing individual high-value payments.

Corporate treasury systems generate payables files with payments which are then released electronically by an employee with approval authority working in treasury. However, this system of internal controls often breaks down. The majority of corporations do not have any controls in place to track who touches the payables file between its

### Guardians of the global system

Today, most digital identities are issued based only on user supplied information. Thus, a fraudulent digital identity can be created since it is not authenticated against other information when it is issued or validated each time it is used. Financial institutions, as the guardians of the global financial system, must be a driving force in improving the identity authentication process and expanding the use of multi factor authentication. With information that they are regulated to protect, i.e. name, address, account numbers, birth date, mother's maiden name, etc. they can authenticate the individual before issuing a digital identity, and then perform real time validation of the identity, in conjunction with a smart card/token, each time it is used. In this way the most current status of the identity is maintained and assurance is provided by the issuing institution to all others relying upon it to complete a transaction.

CORPORATE BOARDS OF DIRECTORS ARE BECOMING INCREASINGLY CONCERNED ABOUT LIABILITY AS A RESULT OF NEWS STORIES OF EMPLOYEE FRAUD, CORPORATE IDENTITY THEFT, COMPUTER BREACHES AND MALFEASANCE.

release from their ERP or treasury system and its transmission to the bank. Additionally, system passwords are scribbled on Post It notes and adhered to treasury workstations so that if the approver is unavailable, another employee can log into the system to release payments and meet the bank's daily cutoff time. Multiple employees using a "communal" logon and password to authorise payments create a murky audit trail.

When processing runs smoothly, employees can provide transaction history, sufficient organisational transparency, tracking of financial transfers and supporting documentation. However, those same corporations stumble when providing historical data for exception processing and to meet changing regulations. Proving compliance during an audit can be challenging and accountability limitations increase financial risk to both the corporations and the banks serving them.

There are additional problems with control: when a corporate treasury department transfers bank payments, most bank systems only verify access and do not validate the actual identity of the employee using the logon and password. To fully protect against identity fraud, corporations need to authenticate the identity of the person accessing the system. Although many corporations issue one-time-password tokens or digital certificates or have implemented site key verification, very few authenticate the user before issuing the credentials. Without individual identity authentication, companies cannot trust that the person accessing the system is actually the party who should have the access credentials.

Without individual identity authentication there is no individual accountability. To provide individual accountability, identity authentication must be integrated into key parts of the corporate treasury workflow. Identity needs to be authenticated before anyone receives a logon, regardless of whether it is a single sign on or is provisioned for rights to or within a system. Identity should also be authenticated prior to allocation of a one-time-password or other token/smart card. Once provisioned, each action taken should be tied to the individual to provide end-to-end accountability.

By not tying individuals to the work they do and the transactions that they generate, corporations can miss behavior and activity patterns that could identify potential fraud. Tracking and accountability per individual must be enterprise-wide and comprehensive.



## AUTHENTICATION OF ALL IDENTITIES PRIOR TO GRANTING ACCESS OR APPROVAL IS A CRITICAL PART OF A COMPREHENSIVE APPROACH TO INTERNAL CONTROLS.

**INDIVIDUAL ACCOUNTABILITY** Today, individual accountability is tied to system logon and activities performed under that logon. However, accountability for the approved bulk files of payments (more than one payment) is available only at the corporate level. This lack of individual identification is true of most information transferred in files rather than individual transactions (e.g. electronic invoice files). Individual accountability for these files, where each signature is at an individual rather than company level improves internal controls. In this way, payables files passed from an ERP or treasury application are tracked with an individual signature all the way through receipt at the financial institution, providing a complete audit trail.

**COST OF UNAUTHORISED ACCESS** As the commercial market continues to expand both business and commerce electronically, investors want reassurance that internal controls are in place. The spectre of unlimited liability in the event of an unauthorised access by either an employee or a hacker is a deterrent to further funding which in turn limits growth and competitiveness. Authentication of all identities – whether internal or external – prior to granting access or approval is a critical part of a comprehensive approach to internal controls. It eliminates the need for corporations to maintain multiple authentication methods for communications both internally and with their financial institutions and limits liability. It also expedites the processing flow and reduces risk since authentication is based on a single identifier. This standardised approach to identity authentication is another step toward expanding straight-through processing (STP). Individual identity signing of all actions, whether payment-related or not, provides a complete end-to-end audit trail. This increased level of accountability enables better regulatory reporting and comprehensive audit tracking across the entire transaction flow from initiation through completion. This in turn expands the transparency needed for liability protection.

John Bullard, Vice President, Global Ambassador, IdenTrust.
**John.Bullard@IdenTrust.com**
www.identrust.com