IdenTrust™

The Payment Factory: Strengthening Compliance and Improving Internal Controls for Corporate Treasurers

White Paper

TABLE OF CONTENTS

INTRODUCTION

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 recognize the challenges of change and embrace them.

Moving to a centralized treasury function—a Payment Factory--is one such change that many are slow to implement even though corporations around the world recognize the benefits that a Payment Factory can bring to their business.

By replacing the current environment of decentralized 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 decentralized treasury to a group or centralized treasury operation. To make this organizational 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.

Centralizing 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. Centralizing 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 U.S. regulators and develop and implement appropriate corporate internal controls. The 8th EU Directive includes parallels to the Sarbanes Oxley (SOX) legislation in the U.S. 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 suite. 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.

Although the list of countries implementing SOX-like controls remains small, the trend is clear: internal controls are becoming more important in the minds of both the regulators and the companies operating within those countries.

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. For example, U.S. retailer TJ Maxx recently agreed to pay a $40.9 million settlement to Visa issuers relating to a computer security breach in which over 94 million Visa and MasterCard accounts and possibly customer driver's licenses may have been exposed.

Media coverage of stories such as the TJ Maxx lawsuit heightens corporate awareness. 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 authorization validation before approving and releasing individual high-value payments.

Corporate treasury systems generate these payables files which are then released electronically by a treasury operator with approval authority. 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 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 authorize payments create a murky audit trail.

When processing runs smoothly, employees can provide transaction history, sufficient organizational 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.

IdenTrust: Individual Accountability

Today, accountability for bulk files of payments (more than one) is only available at the corporate level. The IdenTrust value proposition enables these bulk files to utilize a unique, internationally interoperable capability that provides accountability by identifying each signature at an individual rather than company-level. IdenTrust's open standards-based, proprietary process for identity authentication and validation, the Rule Set, was developed by, and for, the global financial services community and its customers. The Rule Set provides a binding legal and regulatory framework that creates an interoperable identification and authentication process for all transactions and documents.

The IdenTrust Rule Set automates three key activities:

Authenticate – Prove the identity of individuals or businesses.

- IdenTrust identities allow individuals or businesses to prove that they are who they say they are, and conversely, allow individuals or businesses to rely on that proof.
- Because IdenTrust identities are backed by banks around the world, individuals or businesses that rely on that identity are covered by a liability structure provided by the banks (similar to the structure provided in the credit card industry) even if the identity is proven false.

Encrypt – Control visibility into and integrity of transactions or documents.

- IdenTrust identities lock the contents of a transaction file and/or document, making them impossible to tamper with.
- IdenTrust identities can also scramble information, making it impossible to read or decipher by an unauthorized person.
- IdenTrust identities also encrypt and control process flows, eliminating both phishing and man-in-the-middle attacks by ensuring that no one can intercept or redirect the transaction or document.

Digitally Sign – Create a legally binding and non-repudiable electronic signature.

- IdenTrust identities can be used to replace "wet" signatures so electronic documents and transactions have the same levels of legal protection and enforceability associated with traditional ink-based paper signatures.
- Global legal interoperability results from a closed contractual system that governs:
  - Liability and recourse among all parties (a certificate authority (CA) confirms to the relying party (RP) that the subscriber's certificate is not revoked – reducing repudiation risk)
  - Legal recognition of digital signatures
  - Electronic contract formation
  - Dispute resolution over signature validity

Using these three functions alone or in combination, corporations can hold individuals within their organization accountable for creating, transferring, reading or discarding transactions--from signing contracts to initiating payments to handling complex supply chain transactions. This entire process is fully compliant with U.S. regulatory requirements such as Sarbanes Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Financial Institutions Examination Council (FFIEC) multifactor authentication banking guidelines and global initiatives such as anti-money laundering (AML), the Single European Payments Area (SEPA) identity authentication guidelines and Know Your Customer (KYC) requirements around the world.

The IdenTrust PLOT

Although technology issues typically receive the most attention in the identity industry, in reality they represent just the tip of a very large iceberg. The most pressing identity dangers exist in the policy, legal and operations areas. The IdenTrust Rule Set is unique because it focuses on all aspects of identity rather than only on the technology.

IdenTrust PLOT Uniquely Identifies Individual Originators/Receivers of All Types of Files

- Only the total combination of the PLOT components--Policy, Legal Frame work, Operations and Technology--provides a comprehensive approach to identifying the originator and receiver of payment and other types of electronically transferred files.
- Policies and procedures developed and agreed to by financial institutions around the world provide a comprehensive approach to authenticating and issuing these identities.
- IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Other systems require public law for digital signatures to be effective.
- All transaction details remain private; only certificate information is validated.
- Customer agreements are valid, binding and enforceable in countries around the world.
- IdenTrust delivers a complete hosted environment to enable a full spectrum of trusted identity services.
- A single, interoperable identity accepted by multiple financial institutions across multiple applications supports more than just simple file transfer.
- The financial institutions which formed IdenTrust cooperatively defined and developed a standard for authenticating identities that uses the "Know Your Customer" regulations in use in most countries and ensure global enforceability since the digital identity certificate contracts are legally binding

The IdenTrust Rule Set

The IdenTrust Rule Set governs:

Policy issues such as who receives the identity and how each individual or business is vetted to guarantee they really are who they say they are and ensuring that the process is done consistently everywhere around the world.

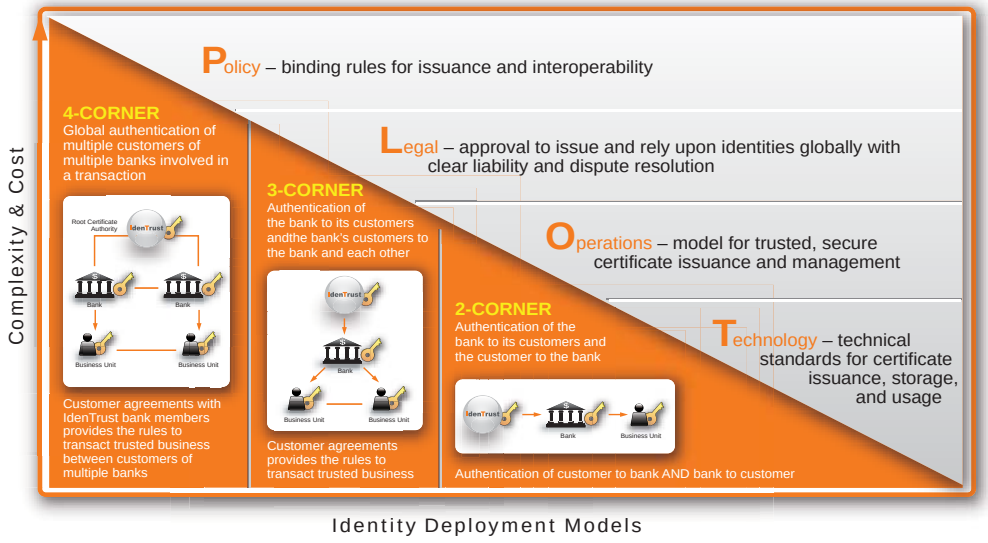
Legal issues such as what should be done when something goes wrong, setting base liability structures and guaranteeing that each identity meets the legal requirements of every jurisdiction.

Operations issues such as how identities are manufactured to ensure that the entire process is secure. This includes physical security (identities are distributed and turned out using at least two different channels such as mail and email or mail and phone) and ensuring that the network is always available.

Technology issues such as the workings of the identities and the overall network. IdenTrust uses standard technology in a unique, proprietary manner to ensure even higher levels of security.

This combination of policy, legal, operations and technology (PLOT) supports more than 40 million transactions annually. These volumes are increasing 15% each month and include financial transactions such as payments as well as business transactions such as invoice flows.

PLOT works in three identity deployment models: a 2-Corner Model in which a corporation interacts only with their own bank; a 3-Corner Model in which a corporation interacts both through their own bank and another customer of that bank; or a 4-Corner Model in which a corporation interacts with multiple banks that are members of the IdenTrust community.



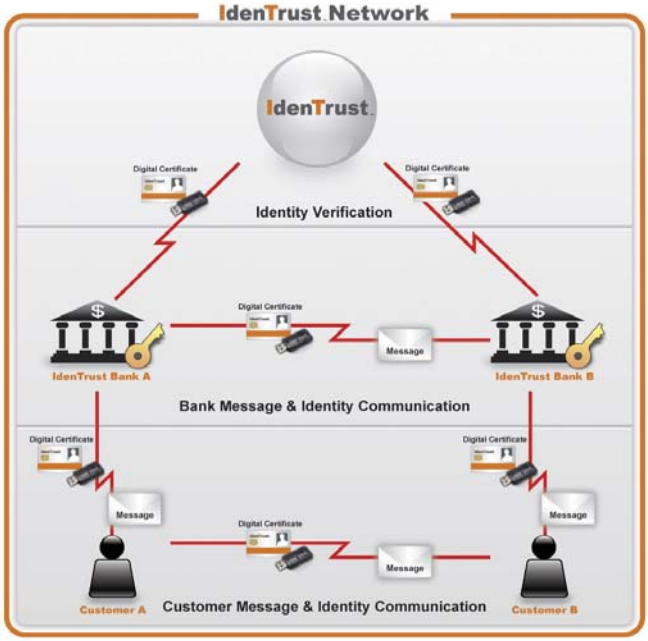
Security and Privacy Combined

Many organizations around the world use digital certificates and access tokens/software that provide high levels of authentication and validation. However, these organizations store the digital certificates and access tokens/software as part of the transaction data. As transactions are opened to perform authentication and verification, privacy is compromised.

IdenTrust does not violate the privacy of the sender or the receiver.

The IdenTrust Rule Set governs the operation of the IdenTrust Trust Network by specifying how a digital identity certificate can be issued and how it is validated. Inherent within the IdenTrust infrastructure and Rule Set is protection against unauthorized access to the transaction information: the IdenTrust infrastructure validates the certificates and only authorized users can interrogate the transaction data.

The transaction data and signed certificate are exchanged between the banks involved in the transaction. The messages related to the transaction data are exchanged between the bank customers on either end of the transaction. IdenTrust only validates the identities used by these customers, not the data associated with the transaction. The transaction data itself is never passed to IdenTrust. It remains with the banks involved.



Summary

As the commercial market continues to expand both business and commerce electronically, investors want reassurance that internal controls are in place. The specter of unlimited liability in the event of an unauthorized access by either an employee or a hacker is a deterrent to further funding which in turn limits growth and competitiveness. Bank-supplied 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 standardized approach to identity authentication is another step toward expanding Straight Through Processing (STP).

IdenTrust enables individual identity signing of all actions, whether payment-related or not, providing a complete end-to-end audit trail. The Rule Set on which the IdenTrust framework operates uses globally accepted Know Your Customer (KYC) guidelines to authenticate the identity, ensuring that the user's identity is authenticated and validated before access is granted. This increased level of accountability enables better regulatory reporting and comprehensive audit tracking across the entire transaction flow from initiation through completion. IdenTrust expands the transparency needed for liability protection.

Authenticating and validating each individual provides bulk file transfers with an additional level of tracking and improves risk controls and regulatory compliance for corporations worldwide. IdenTrust helps financial institutions and their customers expand trust to all types of files and other communications over the Internet while still maintaining privacy. This prevents identity and other types of fraud, makes compliance easier and strengthens authentication which reduces the need for further regulation.

ABOUT IDENTRUST

IdenTrust is the global leader in trusted identity solutions, recognized by global financial institutions, government agencies and departments, and commercial organizations around the world. IdenTrust enables organizations to effectively manage the risks associated with identity authentication; work interoperably with countries around the world; minimize investment in creating their own policies and legal frameworks; and deploy a spectrum of products insuring trust, smarter, faster, and more cost effectively.

The only bank-developed identity authentication system, IdenTrust provides a unique legally and technologically interoperable environment for authenticating and using identities worldwide. The IdenTrust Trust Infrastructure is predicated on a proprietary framework that combines policies, legal framework, trusted operations and technology (PLOT) to create a comprehensive environment for issuing trusted identities. IdenTrust is the only company to provide a solution incorporating all four of these elements. Customer agreements are valid, binding and enforceable in more than 175 countries. IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Competing offerings, in contrast, require participants to navigate a confusing maze of public laws that vary from jurisdiction to jurisdiction. Additionally, the IdenTrust Trust Infrastructure maintains the privacy of each and every transaction processed by reading only digital certificate information, not the message itself.

Additional information can be found at www.IdenTrust.com.

Corporate Headquarters
IdenTrust Inc.
55 Hawthorne Street, Suite 400
San Francisco, CA 94105
USA
Telephone: +1.866.IDENTRUST (+1.866.433.6878)
Fax: +1.415.486.2901
www.IdenTrust.com

European Office
IdenTrust Inc.
288 Bishopsgate
London, England EC2M 4QP
United Kingdom
Telephone: +44 (0)203.008.8330
Fax: +44 (0)203.008.8331