



# **Secure Healthcare Banking: The Critical Step of Identity Verification**

A Whitepaper from Personix

This document is the property of and is proprietary to Personix. It is not to be disclosed, in whole or in part, without the express written authorization of Personix. It shall not be duplicated or used, in whole or in part

© Copyright 2006 Personix, All Rights Reserved

## Overview

Online authentication methods, no matter how sophisticated, are useless in preventing fraud unless the identity of the user has been verified to a reasonable degree of certainty before sign-on credentials are issued.

Medical costs are increasing, and healthcare payers and providers alike are searching for ways to reduce their administration costs. One outstanding example of cost savings is healthcare banking, which integrates healthcare payment processes with network access to the banking infrastructure to lower administrative costs. But online security is an issue, especially when using Electronic Funds Transfer (EFT) to deposit payments into a healthcare provider's bank account. To improve security, there has been significant industry and regulatory emphasis on stronger authentication methods that use multiple identity factors at time of sign-on. Yet insufficient attention is being paid to proving the identity of a provider, and the authenticity of the information they provide, before sign-on credentials are issued. Furthermore, the online sign-up processes typically used to collect the bank account information required for EFT transactions increase the opportunity for both identity and account theft. Simply put, multi-factor authentication at sign-on is insufficient to ensure security for healthcare banking. Multi-factor identity verification during account origination must also be implemented before the security of online financial transactions can be significantly improved.

### The Industry Problem

#### The Soaring Costs of Healthcare

Healthcare costs continue to skyrocket. They accounted for 15.3% of U.S. gross domestic product (GDP) in 2004 and are projected to grow to 20% of GDP by 2015. At over \$2 trillion in 2006, America's health care costs have risen at twice the rate of inflation since 1970 and are currently outpacing the growth of the American economy. In response, healthcare payers (such as insurance companies) and providers (such as physicians and hospitals) have implemented a variety of information technology initiatives to reduce their administrative costs while simultaneously improving patient service and satisfaction.

#### The Promise of Healthcare Banking

One of these industry initiatives is healthcare banking, whose goal is to integrate a wide range of healthcare administrative operations using the existing banking infrastructure, including the use of the Automated Clearing House (ACH) network for electronic funds transfer (EFT) payments to healthcare providers. While automating payments can reduce errors and decrease the time

it takes providers to receive payment, it also introduces new opportunities for fraud, such as identity theft and account theft.

#### Account Theft – A Different Way to Steal Identity

Identity theft isn't limited to individuals. It can happen to companies as well.

Individuals are usually worried that someone will steal their identity to charge unauthorized purchases to their credit cards or take money out of their bank account. And everyone worries that their online credentials (such as user ID and password) may be stolen to allow unauthorized access to important personal accounts. Account theft, while a form of identity theft, is a little different. Instead of taking money out of someone's account, it's stolen before it gets there.

How? The thieves pretend to be the legitimate recipient of the funds. They collect payments that are rightfully the provider's by illegally intercepting their payments before they receive them.

**Corporate identity theft is a little different – instead of taking money out of your account, it's stolen before it gets there.**

This kind of fraud is usually perpetrated by employees of both payers and providers, who take advantage of their intimate knowledge of their employer's business. As employees, they know how to exploit weaknesses in a company's business processes, which makes it even more difficult to detect and prevent their illegal activity. And small healthcare providers are just as, if not more, vulnerable as large corporations.

In fact, dishonest employees at a healthcare payer could create accounts "on behalf of" multiple providers, and could perpetuate fraud on a huge scale in just a few days.

### Motivation for Change

#### White Collar Crime Is Growing

The term "white collar crime" is commonplace, but what is it exactly? Simply put, white collar crime is an illegal or unethical act that violates accepted accounting principles, fiduciary responsibility, or public trust. These include fraud, forgery, and embezzlement, all of which are involved when electronic payments are illegally diverted

as a result of identity and account theft. Regardless of its form, white collar crime is growing and no company is immune, large or small.

Compounding the threat of white collar crime is the Internet, which can allow fraud to be conducted on a grand scale.

#### New Regulatory Mandates

Corporate financial misconduct, identity theft and inappropriate access to personal data have resulted in a growing number of government and industry regulations to combat fraud. Two of these, the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Financial Institutions Examination Council (FFIEC) Guidance, outline security standards designed to protect both payees and payers who utilize healthcare banking services.

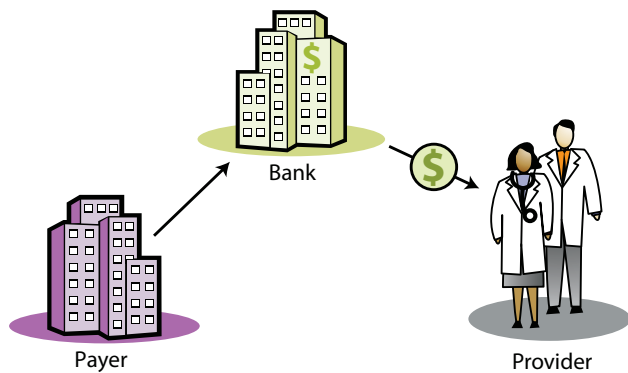
For example, HIPAA requires organizations to maintain a secure infrastructure that controls access to systems that contain protected health information (PHI), including payment information. Similarly, the FFIEC has issued guidance regarding controls necessary to authenticate the identity of customers accessing online financial services.

The FFIEC has issued a guidance titled, "Authentication in an Internet Banking Environment," that calls on banks to upgrade to stronger forms of authentication by the end of 2006. The FFIEC further expects banks to use effective methods of both authentication and identity verification, based on an assessment of risk, when verifying online customers. While not legally mandated for the healthcare industry – yet – these guidelines provide words of wisdom for entities beyond banks, such as providers of healthcare banking services that authenticate users involved in the movement of funds.

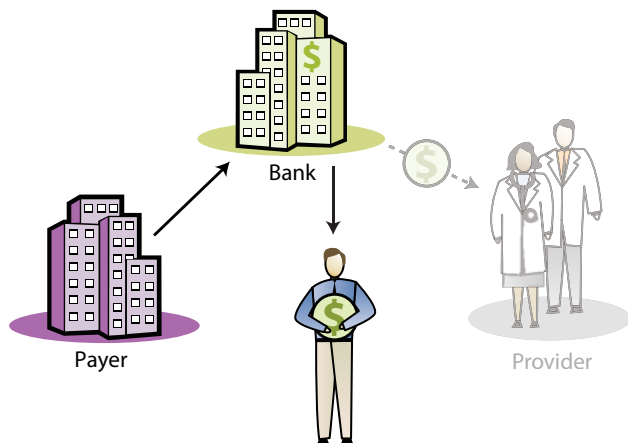
According to this FFIEC guidance, "Customer identity verification during account origination is required by section 326 of the USA PATRIOT Act and is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. Potentially significant risks arise when a financial institution accepts new customers through the Internet or other electronic channels because of the absence of the physical cues that financial institutions traditionally use to identify persons."

Thus far, authentication has garnered the lion's share of attention, but identity verification is equally, if not more, important.

#### Proper Transaction



#### Fraudulent Transaction



**Unfortunately, weak identity verification processes allow an employee to falsify their identity and provide fake bank account information that can divert all future deposits into an account they control.**

### How Account Theft Begins

Today, using electronic funds transfer (EFT) to directly deposit payments to a recipient's bank account has become commonplace. But whether the recipient is a healthcare provider or a member (e.g., subscribed individuals covered under the applicable health plan, or participating in Consumer-Directed Health Plans), they must first provide their bank account information to the payer as they set up their payment details at account origination.

Unfortunately, the processes that are typically used to collect this information present opportunities for healthcare payers and providers to be victimized on a massive scale by identity thieves. Regardless of whether registration occurs online or using traditional methods, the primary issue remains to prove the authenticity of the bank account information provided and the person who provided it.

Traditionally, accounts of all kinds have been originated manually. For example, forms are mailed or faxed to the healthcare provider or member to be filled out and returned. Alternatively, the needed information is collected over the phone by the payer or their healthcare banking service. These manual processes are certainly vulnerable to fraud, since it's possible to provide false information on the forms or over the phone – but they are less vulnerable than a fully-automated process with no identity verification procedures in place.

But, payers recognize that these manual processes are time intensive and cost prohibitive. In their efforts to improve the adoption rate of healthcare banking by healthcare providers, payers have attempted to make sign-up processes as user-friendly and fast as possible. As a result, most provider bank account information is now being obtained via the Internet – but the outmoded online security methods that they typically use are extremely vulnerable to fraud. In the older manual account origination process, a human being has the opportunity to review and check out the data being provided. But in an automated sign-up process without strong identity verification procedures built in, the possibility for fraud on a large scale increases dramatically.

Weak online identity verification processes allow employees to falsify their identities and provide fraudulent bank account information at EFT account origination, and then divert all future deposits into an account they control.

The best authentication processes in the world won't protect against this threat – though strong authentication is essential to provide a secure solution. To implement

a comprehensive solution, both providers and payers must ensure that they fully understand the capabilities, strengths, and limitations of authentication procedures as well as identity verification solutions.

## Authentication vs. Identity Verification

### Authentication vs. Identity Verification

User authentication is not the same thing as identity verification; rather, both are separate steps in a vital process to secure the electronic transfer of funds. While the distinction between the two is subtle, it is critically important. Authentication merely proves that the user can provide one or more forms of identification that match what the system expects. Identity verification establishes that an individual is who they claim to be. Simply stated, the strongest authentication system is useless unless the healthcare banking service can verify an individual's claimed identity before they are issued sign-on credentials.

### Requirements for Secure Authentication and Identity Verification

To date, authentication has been the main focus in protecting online accounts. However, achieving a comprehensive process for securing healthcare banking details consists of three components:

- » User identity verification when registering for direct payment deposit
- » Bank account validation at the time of EFT account origination / registration
- » User authentication at time of sign-on

The absence of even one of these creates significant opportunities for identity or account theft, and can result in embezzlement or other forms of financial fraud. Sadly, while a lot of attention is paid to different ways of authenticating a user at sign-on, verifying a user's identity at account origination is only beginning to garner industry recognition.

## Authentication Alone is Insufficient

### Authentication

Authentication is designed to establish that a person attempting to gain access to an account or information is the person who set up the account. We authenticate ourselves every day when we log in to a website with a

**“Potentially significant risks arise when a financial institution accepts new customers through the Internet or other electronic channels because of the absence of the physical cues that financial institutions traditionally use to identify persons.”**

FFIEC Guidance,  
“Authentication in an Internet  
Banking Environment”

user ID and password, enter a PIN to use our ATM cards, or verify our mother’s maiden name when we call in to our insurance company, phone company, or bank. In each case, we provide information that the company matches with details supplied when the account was created (account origination). Strong authentication processes are vital in protecting our increasingly-automated accounts.

### **One Factor, Two Factor, Multifactor Authentication**

The number and variety of authentication technologies and processes is bewildering. They include passwords, personal identification numbers (PINs), challenge/response prompts, digital certificates, physical devices such as smart cards, one-time password (OTP) generators, plug-ins or other types of “tokens”, and biometric identification.

Some of these authentication mechanisms use arcane and complex technologies, many of which are difficult to implement and expensive to administer. But in general, all of these methods have one thing in common – they require the user to present at least one of the following authenticating factors to prove their identity:

1. **Something a person knows** – a secret, such as a password, a personal identification number (PIN), or an answer to a personal question. If the user types in the correct password, PIN or answer, access is granted.
2. **Something a person has** – a token, such as a physical device (e.g., smart card, hardware token, digital certificate). The user physically possesses something that contains their authentication credentials and often requires using either specialized hardware or software.
3. **Something a person is** – a biometric, such as a physical characteristic or some unique attribute of the individual, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the eye.

The use of two or more authentication methods at the same time is generally referred to as multifactor authentication. There are many different ways to implement multifactor authentication and some are better suited for some situations than others. But in general, the most common type of multifactor authentication is to use two independent ways to authenticate identity and assign privileges based on that identity. This process is similar to being asked to show two forms of identification when cashing a check or applying for a passport.

Every authentication method has inherent limitations and any security system – no matter how strong it may be – can be compromised, including multifactor authentication. But regardless of how many authentication factors are implemented, they are all equally useless in preventing fraud unless the authenticity of the user’s identity has been previously verified.

### **Current Authentication Solutions and their Weaknesses**

In today’s world, we not only rely on technology, we take it for granted. This is particularly true when it comes to online fraud prevention. The problem with relying on authentication technology for preventing fraud is the flawed assumption that the individual using the technology is actually who they claim to be.

The fact is that most authentication methods fail to verify the identity of the individuals when they initially register for their online user ID and password. All too often, their claimed identity is taken for granted and never challenged. In reality, the effectiveness of any given authentication solution is highly dependent not just upon the integrity of the technologies they use, but also how they are implemented and managed.

## **Identity Verification – The Missing Step**

### **Identity Verification**

While we’d all like to believe that people are who they claim to be, the reality is that healthcare payers need to be on the defensive against unscrupulous individuals who would steal a provider’s identity for criminal purposes. Part of that defense is to know with demonstrable certainty that the people they deal with on a daily basis – in person or online – are really who they claim to be.

The first step in establishing the authenticity of an individual is to validate, with as much assurance as is reasonably possible, that they are who they claim to be before authentication credentials are issued to them. Unfortunately, this key point seems to be overlooked far too often for comfort.

The certainty of authenticating individuals online should closely resemble that achieved when individuals walk into a bank and are required to provide evidence that they are who they claim to be and that they are customers of the bank.

The certainty of authenticating individuals online should closely resemble that achieved when individuals walk into a bank and are required to provide evidence that they are who they claim to be and substantiate they are customers of the bank.

## Current Approaches to Identity Verification

### Current Identity Verification Methods and Their Weaknesses

Healthcare banking services currently use a variety of methods in their attempt to verify the identity of a user and validate the authenticity of the bank account information they provide. On the surface, some of these may appear to offer adequate security safeguards. But under careful scrutiny, each one has inherent flaws and associated exposure to risk, which are often downplayed to promote a false sense of security. For example:

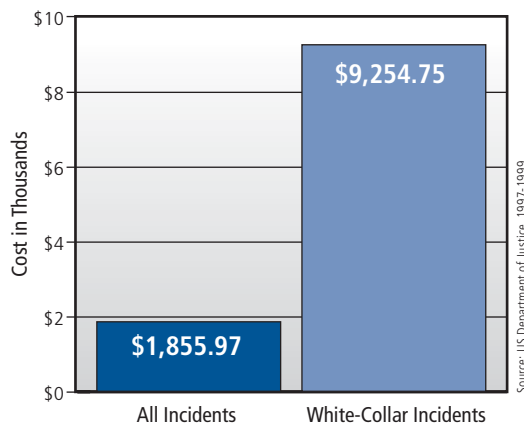
1. **Pre-notes** – A pre-note is simply an electronic way of verifying the existence of a bank account. It works by submitting a zero-dollar sum EFT transaction from the payer’s bank, through the banking network, to the recipient’s bank account as specified by the provided routing and account numbers. If the pre-note is sent to an invalid account number (e.g., the specified account does not exist), the payer’s bank will receive notification. If the pre-note is sent to a valid account number, no notification is sent to the payer’s bank. It’s important to understand that a pre-note transaction does not validate who owns the account, only that it exists. Therefore, a pre-note would fail to offer any protection if a dishonest employee attempted to embezzle funds by registering a bank routing and bank account number different than their employer’s. Furthermore, use of a pre-note won’t reveal the identity of the employee. While standard auditing and tracing mechanisms would eventually detect that fraudulent activity took place, it would likely be only after funds had already been misdirected and may not be recoverable.

- 2. **Calling banks** – Some healthcare banking services may assert that they initiate a call to the payee’s bank to confirm account ownership of the bank routing and account number provided by the payee for receipt of EFT payments. However, due to financial privacy regulations, a financial institution will likely neither confirm nor deny whether the bank account name is associated with a provided bank routing and account number. Therefore, calling the bank to confirm the ownership of an account name and associated routing number will not likely deter fraudulent activity. Other, more involved methods should be used to validate account ownership.
- 3. **Small EFT credits** – Another approach to verifying bank account ownership is to make one or more very small EFT credit transfers (e.g., two cents, eleven cents, etc.) into the registered bank account. The bank account owner is then contacted and asked to verify the amount of each deposit. However, if a provider’s employee originally registered the routing and account number to themselves, then making deposits and requiring the employee to validate the amount of those deposits would fail to offer protection against fraudulent transactions.

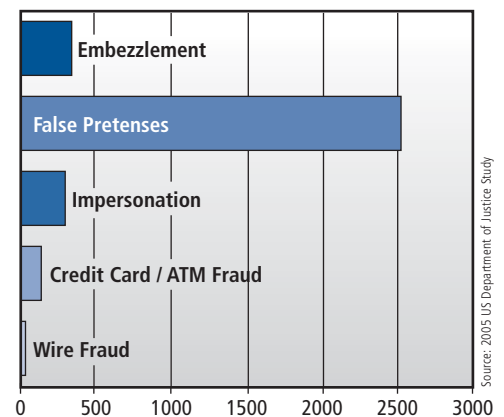
Unfortunately, none of these methods adequately verifies the true identity of the user. Instead, they merely validate that the banking information provided is capable of routing and electronic deposit to an account.

The good news is that better methods exist to verify a user’s identity and validate the authenticity of an account. Experienced providers of healthcare banking services, such as Personix, have proprietary, multi-step processes to ensure the security of healthcare payments.

**Average Cost of Property Lost due to Criminal Acts**



**Number of White Collar Crimes Committed in Doctor’s Offices**



## New Approaches to Identity Verification

### Out-of-Band Identity Verification

Fortunately, a well-proven process exists for certifying the true identity of the individual at the time of online registration. Used for many years in the commercial banking and brokerage industries, “out-of-band” validation provides the additional identity verification step that is generally missing in the authentication methods used in healthcare banking registration and enrollment processes.

Broadly speaking, out-of-band identity verification includes any technique that allows the identity of the individual to be validated through a channel that is different than the one that will be used for authentication. As in multifactor authentication, some techniques are better suited for certain situations than others, generally based on the desired level of risk mitigation.

### Requiring Multiple Proofs of Identity

As it applies to healthcare banking, out-of-band identity verification requires the use of one or more different forms of communication during the healthcare provider registration process. When combined with multiple validation factors, it can significantly improve the certainty of verifying an individual’s identity while simultaneously mitigating the risk of account theft. For example:

- » Instead of registering the healthcare provider entirely online, they are either contacted in person or by phone, FAX, email or surface mail
- » Each time they are contacted, a different communications method is used
- » Likewise, a different proof of identity is requested at each step

With each step, the odds of the enrollee being who they claim to be are increased by requiring them to provide more than one form or identity validation. Once their identity, and the bank account information they provide, has been validated to an acceptable degree of certainty, they are issued sign-on credentials. Should the healthcare provider’s registered banking information change, the identity and account verification process is repeated.

## Authentication and Identity Verification Solution Considerations

### Balancing Risk and Security

No security technology or process, regardless of the technology it uses, can eliminate the possibility of fraud or embezzlement with absolute certainty. The objective is to provide a reasonable level of safety with sufficient controls to diminish its potential. In general, the degree to which an authentication system relies on prior verification of a person’s identity is determined by balancing the amount of risk that is tolerable and the cost or effort required to gather additional identity validation.

However, the authentication technologies and identity verification methods selected should be appropriate and reasonable for the risk associated with a given application. For example, high-risk processes such as financial transactions should require a verification procedure to establish, with some degree of confidence, the identity of the user at the time of registration for EFT healthcare banking services.

### Usability Requirements for Industry Adoption

We live in a culture of convenience and instant gratification. If we can’t get it quick, simple, and user-friendly, we become impatient and lose interest. Authentication and identity verification processes that fail to meet these criteria, no matter how beneficial they may be, will be met with resistance. To be successful, an end-to-end identity authentication solution for healthcare banking must:

- » Pass the usability test
- » Adequately confirm the identity of the user
- » Integrate well into an online user registration process
- » Provide a reasonable cost/benefit ratio

Healthcare banking services require a safe and dependable online registration process to verify the identity of healthcare providers and the authenticity of their banking information. Current online-only enrollment methods are susceptible to a dishonest employee or criminal posing as the healthcare provider and supplying false bank account information. But more dependable identity and account verification processes commonly in use today are time consuming, cumbersome, and require the enrollee to be physically present.

**Used for many years in the commercial banking and brokerage industries, “out-of-band” validation provides the additional identity verification step that is generally missing in the authentication methods used in medical banking registration and enrollment processes.**

Regardless of how many authentication factors are implemented, they are all equally useless in preventing fraud unless the authenticity of the user's identity has been previously verified.

Implementing a viable identity verification process for on-line user registration requires striking a balance between usability and reasonably acceptable validation of the identity of the individual providing the information.

## Summary

### Processes that Minimize Risk

Given the anonymity of the Internet and the inherent weaknesses of most authentication systems, the potential for fraud and embezzlement on a large scale is extremely high. At a large healthcare provider, an employee could divert millions of dollars in a week or two and be retired on a beach in Belize long before the theft is discovered.

Minimizing the risk of fraud and embezzlement in healthcare banking requires processes for both multifactor authentication and out-of-band identity verification as healthcare providers set up accounts and provide banking information for the transfer of funds via direct deposit. Multifactor authentication protects against individuals accessing accounts that they didn't create. Out-of-band identity verification is needed to protect payers and providers against dishonest individuals who supply fake banking information when originating the provider's direct deposit account, in order to divert the provider's incoming payments into an account they control.

The resulting identity verification process must strike a balance between ease-of-use and cost requirements and adequately mitigating relevant risks.

### Secure, Cost-Effective Healthcare Banking from Personix

Financial fraud is a fact of online life. The statistics are sobering and the economic costs, especially for embezzlement, are staggering. Furthermore, the fear of

fraud erodes public trust and confidence and inhibits the number of healthcare providers who otherwise might adopt EFT payments.

Personix understands the importance of both multifactor authentication and multifactor identity verification... and we understand the delicate balance between security and simplicity of account origination and use.

Our MedePay>EFT/EFA solution reduces the potential for online financial fraud by providing a practical and effective method of verifying the identity of healthcare providers, while simultaneously validating the authenticity (in a proprietary and effective way) of the banking information they provide. Based on a multi-step, multifactor approach, Personix's unique processes verify identity in a quick, simple, and secure manner that facilitates healthcare provider adoption of healthcare banking services.

Personix applies its proprietary approach to secure healthcare banking payments in a practical and business-oriented process that is quick, simple, and secure. The result: a secure healthcare payment solution that could potentially save payers millions of dollars in fraud prevention.

We urge you to ensure that your business is taking the necessary precautions – contact Personix today to learn more about how you can cost-effective and secure medical banking solution. For more information on EFT, ERA, and the MedePay>EFT/ERA solution, please contact Personix:

#### Jarvis Shockey

Healthcare Banking Market Manager  
13100 North Promenade Boulevard, Stafford, TX 77477  
319-363-2113  
www.personix.com  
medepay@personix.fiserv.com



For more information visit [www.personix.com](http://www.personix.com)

**Personix Houston** • 13100 N. Promenade Blvd., Stafford, TX 77477, Tel: 800.736.2677, Fax: 281.240.2485

**Personix Indianapolis** • 2307 Directors Row, Indianapolis, IN 46241, Tel: 800.759.6401, Fax: 317.576.6779

**Personix Nashville** • 1826 Elm Hill Pike, Nashville, TN 37210, Tel: 615.889.3170, Fax: 615.889.2526

**Personix St. Paul** • 1880 Park View Drive, Ste 100, Shoreview, MN 55126, Tel: 800.842.4712, Fax: 651.846.3850

**Personix Hartford** • Technology Center, 881 Main Street, Manchester, CT 06040, Tel: 860.643.1925, Fax: 860.643.8069

**Personix Boston** • 200 Financial Park, Franklin, MA 02038, Tel: 508.541.4000

**Personix Direct** • 2465 Centerline Industrial Drive, Maryland Heights, MO, 63043, Tel: 800-467-7799, Fax: 314-991-0101

Personix is a service mark of Fiserv, Inc. Fiserv is a registered service mark of Fiserv, Inc. Other brand and names are the property of their respective owners. Information subject to change.  
© 2006 Fiserv, Inc. All rights reserved.

Another **Fiserv** Connection