

Executive Overview



Innovative technology expands the scope and justification for biometrics from simple password replacement and multi-factor authentication to

Fraud Mitigation

Using Biometrics for Fraud Mitigation:

Biometrics offers much more than just simple password replacement. With unique, innovative technology, biometrics can identify the actual user in "realtime" and grant or deny access to critical functions and data. This will help to prevent costly incidents within the system.

bioLock - First System to Protect and Identify:

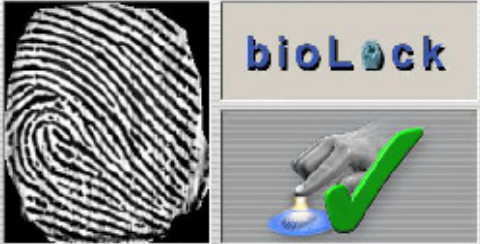
- Protect any mouse click in the SAP application
- Enable fraud mitigation
- Biometric identification of the "actual" user

bioLock – Extra Security for All Critical Areas:

The bioLock system adds a second layer of protection (a biometric "door lock") on any critical area or function of your SAP system. In addition to the SAP User authorization users need a "special invitation" from the bioLock system to execute protected functions.

Common Areas that receive bioLock Protection:

- User Logon
- Finance
- Human Resources
- Purchasing
- Research



biometric verification is required to continue

The Purpose of the bioLock Verification Process:

This process ensures that even authorized users can not commit fraud using other people's user profiles.

For example: If an authorized user, John, tries to make a wire transfer using Peter's SAP user id, his attempt will be rejected, but it will clearly state in the log file that John - uniquely identified with biometrics - tried to attempt fraud with another person's user profile. Thus the fraud attempt was successfully prevented.

Once a transaction or function is requested, such as displaying a balance sheet, creating a purchase order or issuing a wire transfer, the bioLock system will pop up a window requesting a biometric verification. A person's finger has to be placed on the sensor in order to proceed.

bioLock Verification Process:

- The user's finger is placed on the sensor
- Immediately bioLock scrolls through the database templates to find if the finger is registered
- **If the template is not found:** the task **will always be rejected**, even if executed by an administrator with all access rights!
- **If the template is recognized:** the system will then check the bioLock settings with pre-defined special permission settings that indicate the user has authorization from bioLock and will then accept or reject the request
- Executed and rejected tasks will be logged in the log file for auditing purposes

bioLock is a Unique Verification Process for Fraud Prevention:

For the first time, fraud can be identified, prevented, and the attacker can be questioned or even arrested in "real time" since biometrics has uniquely identified the individual within the SAP system. Of course, all critical tasks that John does while being logged in as John will be recorded in the user profile as well. Auditors always have proof of who did what and when in the system and this can help your company to identify, prevent, and deter fraud.



Identification and Conviction is Finally Possible!

Companies lost 7% of their annual revenue to fraud in 2008:

- Median loss for first, single incident was \$175,000
- The average was 7% of the company's revenue or \$994 Billion in the US
- Frauds were most often committed by the accounting department or upper management
- Nearly all intruders were first time offenders (only 7% had prior convictions)
- Occupational fraud schemes frequently continue for years before they are detected

Lack of adequate internal controls was most commonly cited as the factor that allowed fraud to occur. Thirty-five percent of respondents cited inadequate internal controls as a primary contributing factor in the frauds they investigated. Lack of management review and override of existing controls were each cited by 17% of respondents.

Read the full study at: <http://www.acfe.com/RTTN/2008-rtn.asp>

(Source: 2008 Study - Association of Certified Fraud Examiners – www.acfe.com)

Innovative Biometric Technology can help Correct and Secure many Typical Problem Areas:

- **SAP Logon:** Unauthorized users use or share SAP User ID's, even at different locations at the same time
- **HR:** Protect and secure HR information including health insurance, salaries and social security info
- **Finance:** Prevent tampering of payment releases, salaries, wire transfers, requesting or changing budgets
- **Balance Sheets:** Access to any internal company information
- **Research Data:** Research data that is stolen or changed
- **Purchasing:** Unauthorized users purchase unauthorized items
- **Workflow Approval:** People use supervisors password's with or without them knowing about it
- **Fast User Switching:** Users are supposed to log in and out for minimum tasks (bank, hospital, warehouse)
- **Convenience:** Remember multiple passwords that could require up to 15 characters
- **Compliance:** Passwords offer NO True Identity Management (SOX, Section 404, Internal Controls)

20 Ways to get Passwords to any SAP User Profile:

- 82% of all passwords are written down
- 40% of all users share passwords frequently
- Password crackers crack 80% in 30 seconds
- Passwords are not encrypted between computer and SAP system

*Most companies spend more
on coffee than on security!*

The California State University, Fullerton has researched 20 ways to get somebody else's password. Paul Sheldon Foote, Ph.D., Professor of Accounting at the University is leading the research project and has been featured in an SAP TV movie about Sarbanes-Oxley and Pete Gunn in a movie about bioLock at Brevard / NASA ([Link to movie](#)).



Paul Sheldon Foote
Professor of Accounting, California State University

Prof. Paul Sheldon Foote about Passwords:

"Finding passwords on a person's desk, telephoning to ask for a password, packet sniffing, phishing, spoofed (fraudulent) websites, phone phishing, pharming, and vishing are only some of the successful techniques for password fraud. The end of an era of corporate contributory negligence will arrive when corporate leaders accept the responsibility of implementing multiple biometric authentication protocols."

Download the Fishing for Password document to learn how dangerous passwords really are ([pdf](#)).



Kenneth "Pete" Gunn
Director Safety and Security, Florida Space Authority

Kenneth "Pete" Gunn about Passwords:

"Seize the moment and go forward with biometric technology. That is the way of the future, because current systems where you have to develop a pin or a password - that is too expensive and too cumbersome and it is a major weak spot in the security makeup."

View other security comments from Pete Gunn, Paul Foote and others in a 2 minute movie clip ([wmv](#)).

View a Demo of our Fraud Mitigation Approach in the SAP System:

Learn how biometrics can overcome the limitations of passwords and help you to prevent costly fraud within your SAP System:

Streaming Video ([youtube](#)) - wired high-speed access required for best quality

Download Video ([zip](#)) - recommended for better viewing experience and to share

Power Point Demo ([ppt](#)) - view the demo via slides with screen shoots and detailed explanations

Act Now and Fasten Your System's Seatbelt:

When we get into our cars most of us automatically fasten our seatbelts!

Accident statistics, as well as daily news stories, prove that using seatbelts prevents damages. In the industry news, we see companies "being hit" with fraud and the resulting major financial damages on a daily basis. Fraud statistics confirm the dramatic increase! **Fasten your "System's Seatbelt" NOW and act, BEFORE your organization gets "hit"** with major financial damages and bad press! Our innovative security measures can help your company to avoid the loss of significant amounts of time and money, and to also avoid negative impacts on your professional reputation.

Allow us to educate your team further:

Please contact us for any questions and to schedule a personalized, educational demonstration of our biometric identity management and fraud mitigation solution, www.bioLock.us , for your team.

www.fraudmitigation.com

realtime North America Inc. +1-813-283-0070 1-877-bioLock Info@bioLock.us

Copyright 2002-2007 | realtime North America Inc. | All Rights Reserved