

Securing online banking transactions is paramount to the success of our customers' risk management initiatives.

Werner Liebenberg
Account Manager, Johannesburg, South Africa



ACI Online Banking Fraud Management

ACI Enterprise Banker™ and ACI Proactive Risk Manager™

Fraud trends

The banking industry has quickly embraced web-based technology for innovative product offerings and ease of banking across retail and business banking product lines. Along with this proliferation of online banking offerings, quickly comes the need to ensure that all transactions are processed accurately and securely.

According to the participants in a 2010 Ponemon Institute survey, 55 percent of businesses were victims of fraud in the prior year, with 58 percent of fraud enabled by online banking activities. Eighty percent of banks failed to catch fraud before funds were transferred out of their institution. In 87 percent of fraud attacks, the bank was unable to fully recover assets and 57 percent of the respondents that experienced a fraud attack were not fully compensated by their banks. Twenty-six percent were not compensated for any part of their losses.

In addition, the report identified how the fraud had damaged customer relationships with 40 percent of the businesses moving their banking activities elsewhere after a fraud incident.¹

These statistics illustrate the need for agile fraud management solutions in today's banking environment. As the frequency and magnitude of online banking security breaches threaten both consumer and corporate banking, financial institutions are faced with finding ways to protect customer assets and in turn protect their financial health and public image.

A winning combination for online banking fraud detection and prevention

ACI Enterprise Banker™ is the industry-leading online banking system and is used by more large institutions than any other system in the world. The enterprise-wide solution allows financial institutions of all sizes to uniquely package products and services for different markets – or even individual customers – from a single, flexible platform. Enterprise Banker offers a full range of functionality including balance and transaction reporting, ACH and wire transfer origination and reporting, remote check deposit, bill presentment and payment, and cash concentration.

ACI Proactive Risk Manager™ is a complete fraud detection solution which manages risk across a financial

Online banking fraud scenarios

Account takeover and man-in-the-browser (MITB) attacks are two of the most widespread and damaging fraud methods currently impacting the online banking industry.

Recent breaches at an authentication provider and a third-party marketing vendor, coupled with a new generation of Trojan stealth malware, have fostered an attack-rich environment in the banking industry. Events like this have created a supermarket of malware offerings used by fraudsters to access computer systems without users' consent. The new malware can communicate with automated command and control centers in order to remotely self update in an effort to respond to detection attempts by anti-virus programs.²

Account takeover occurs when a perpetrator gains illegal access to a customer's account. Access to the account is gained by stealing authentication credentials. This is accomplished through phishing and other social engineering fraud techniques which aim to steal authentication credentials, as well as malware that specifically captures all keystrokes when the user attempts to log into a secure website.

In contrast, MITB fraud bypasses authentication by using the customer to authenticate. It is conducted using malware like Trojans and Spyware (hidden in email spam scams, PDF files, social networking sites, etc.). The perpetrator allows the customer to authenticate then gains control of the session post authentication unbeknown to the customer. Perpetrators can then initiate new transactions and/or modify existing payments to steal funds.

The rapid evolution of malware programs has kept financial institutions and law enforcement authorities scrambling to educate, inform and protect consumers and businesses about the underground and commercially produced fraudulent toolkits and their related threats and impacts. In the U.S. in 2010, a Zeus botnet operation was busted for siphoning more than \$12.5 million from victims' bank accounts.

1 Ponemon Institute Fraud Survey, March 2010

2 Financial Crime Risk Management Systems 2010: Market Analysis, Chartis Research Ltd., 2010

institution's business lines and customer accounts. Proactive Risk Manager combines the power of advanced analytics, custom neural network modeling and intuitive investigative tools for a fast, accurate and flexible response to current and emerging fraud trends.

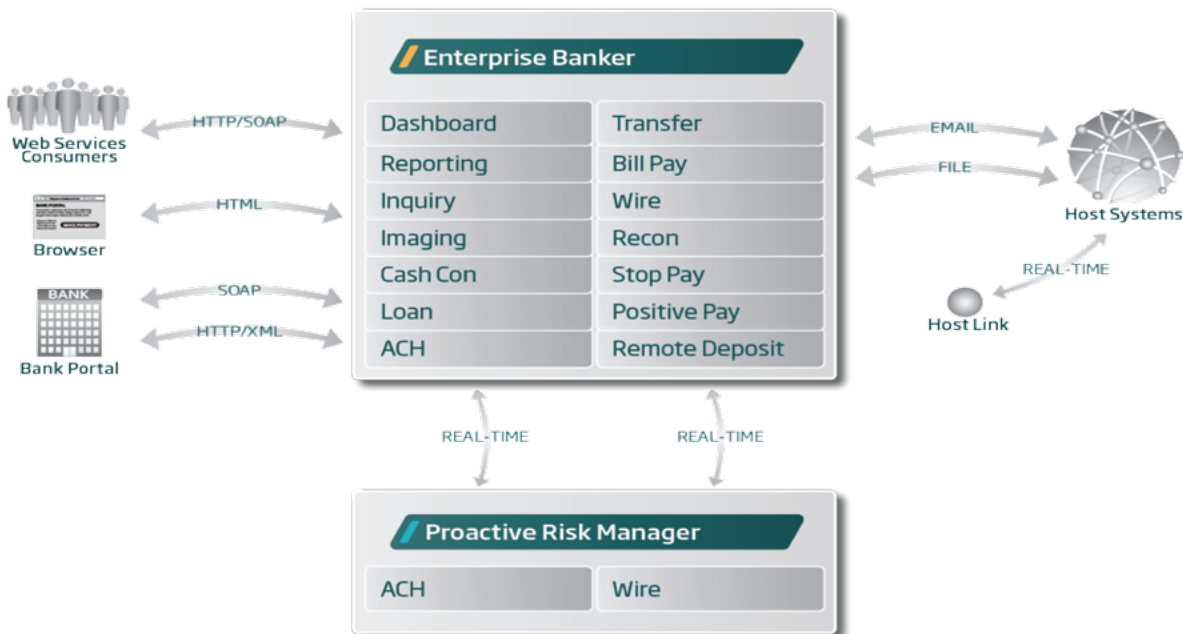
The ACI Online Banking Fraud Management solution offers a system that leverages and closely monitors all Enterprise Banker customer activity, including log-In, expected usage and likely transactions to identify anomalies in behavior that can indicate suspicious activities. Financial institutions have immediate protection for their online banking activities through monitoring and analysis of log-in and token authentication, browser security, entitlements and other security protocols within the core Enterprise Banker offering. By leveraging these protocols and data points, Proactive Risk Manager can identify suspicious transaction activity in real time and stop fraudulent ACH and wire transfers immediately.

With this solution, financial institutions work with a single vendor to securely manage online banking transactions, avoiding the challenges of managing disparate vendor solutions and large data mapping efforts, which end up costing more in time-to-market, deployment, maintenance and product upgrade fees.

Seamless protection from payment experts

ACI combines a global perspective with local presence. Our proven products, domain expertise and 35 years of experience have earned us a position as trusted provider of gold-standard payment solutions.

Enterprise Banker helps institutions reduce operating costs through the use of a single platform for all online banking activities and customers. It enables institutions to offer their customers a variety of packages to meet their unique needs for reporting, payments and online banking services, which encourages customer adoption of online banking and improves customer satisfaction and retention.



→ The ACI Online Banking Fraud Management solution is scalable to support growth in both the number of customers as well as transaction volumes.

Proactive Risk Manager uses sophisticated analytics technology to stop fraud within the transaction authorization path. Its modular architecture allows institutions to create highly tailored packages that meet the specific needs of individual customer types – either by business size, geography or industry niche. The solution is scalable to support growth in both the number of customers as well as transaction volumes.

Enterprise Banker clients now have the ability to seamlessly interface with Proactive Risk Manager to monitor their customers' login, ACH and wire activity through a standard, hosted interface. In real time, ACH batch and wire transactions can be approved, declined or referred based on a set of pre-defined rules.

The package includes a set of analytics and rules specially designed to address current fraud trends in online banking including account takeover and MITB attacks. The combination of Enterprise Banker and Proactive Risk Manager facilitates the security benefits of token authentication, browser security, velocity and limit threshold monitoring, and entitlements along with monitoring expected client behavior and profiling to create a stronger defense for online banking and fraud. The combination of Enterprise Banker and Proactive Risk Manager allows partnering firms to leverage ACI payments expertise, advanced analytics and pre-built functionality to create a stronger barrier to fraud with minimum impact to customer experience.

ACI Analytics and online banking fraud management best practices

The ACI Online Banking Fraud Management solution includes ACI Analytics fraud optimization support and access to ACI's financial crime management expert team including solution and technical consultants. With this offering, ACI offers a review of customers' online fraud management tactics and provides analytics optimization, support and testing.

Based on the input from the financial institution's team of fraud analysts and managers, ACI's financial crime management experts will document and deliver a set of online banking fraud management rules that target suspicious transactions. These out-of-the-box

Transactional monitoring and customer profiling

Because two-factor authentication measures such as tokens are only one layer of protection, financial institutions can further mitigate their risk by monitoring transactional behavior to determine whether or not activity occurring online, such as the initiation of ACH or wire transfers, fits the profile for the genuine customer.

Non-financial information – such as IP addresses, login activities and device characteristics – has become a dominant indicator of fraudulent activity and should be used to create a customer profile. Behavioral profiles store data from past transactions to create a baseline of normal customer activity. Each new transaction is compared to the stored behavioral profile in order to identify deviations. Characteristics of any new payee are compared to other accounts the customer has made payments to in the past.

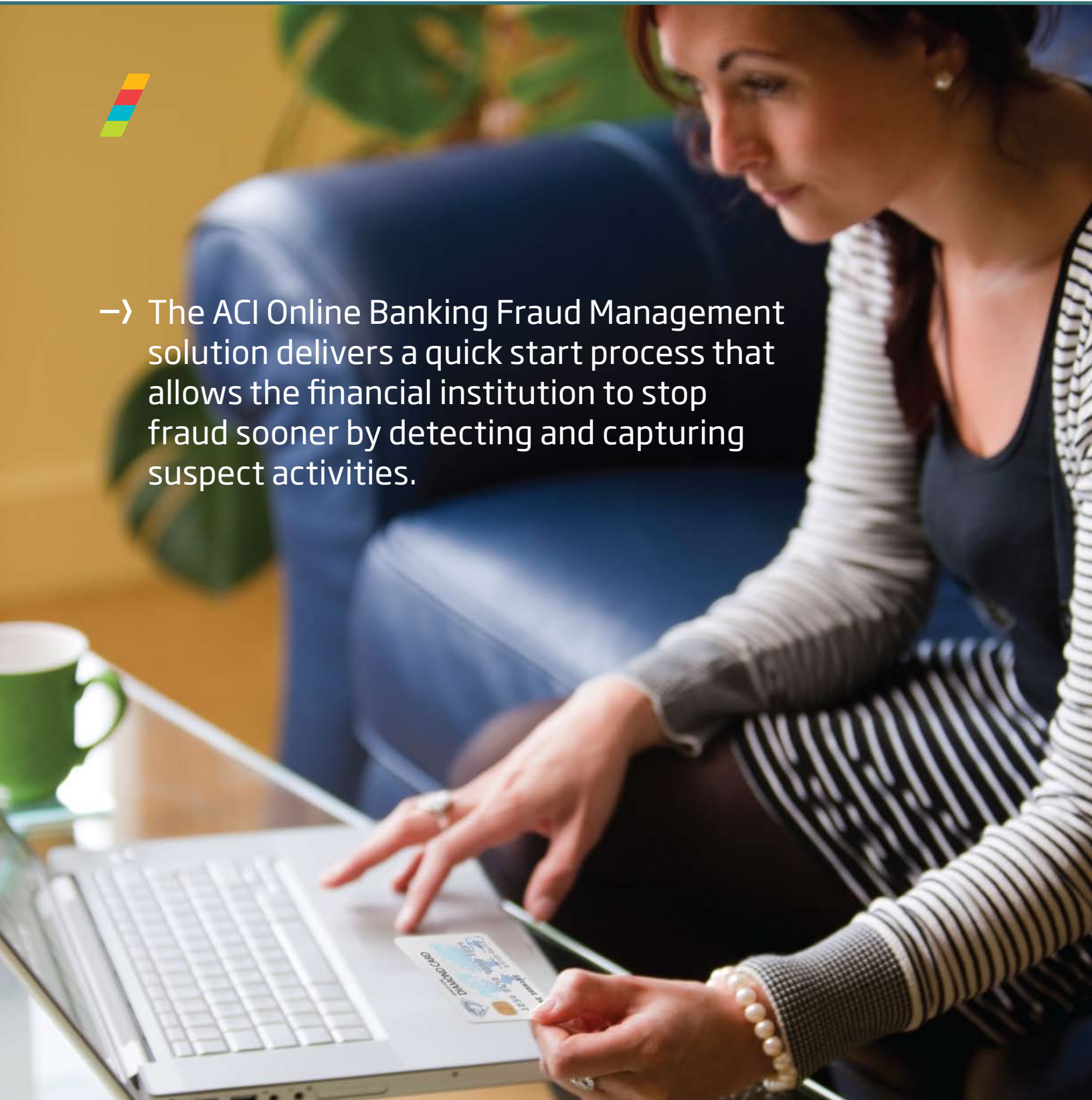
When high-risk activity is detected, action can be taken in real time or near-real time to stop the transfer of funds from the customer's account. Funds can be placed on hold until fraud analysts are able to verify the legitimacy of the transaction by contacting the customer and validating the activity in question.

capabilities will enable the fraud team to quickly start its investigation to determine if an account or transaction may be compromised.

Developed on industry best practices, this process will reduce the amount of rules that financial institutions' analysts need to write, and enable them instead to focus on fine tuning the alert quality. In doing so, the ACI Online Banking Fraud Management solution delivers a quick start process that allows the financial institution to stop fraud sooner by detecting and capturing suspect activities.



→ The ACI Online Banking Fraud Management solution delivers a quick start process that allows the financial institution to stop fraud sooner by detecting and capturing suspect activities.





On demand and onsite delivery options

ACI Online Banking Fraud Management is available in both an on-demand or on-premise capacity.

With the ACI on Demand option, institutions access the ACI Online Banking Fraud Management solution in a secure, redundant and reliable outsourced environment. ACI staff manages and operates the data center and manages ACI Analytics fraud optimization processes, allowing institutions to focus on the core business of servicing their customers. ACI removes the burden of managing hardware, and ACI manages the software upgrade process, so minimal involvement is required from a financial institution's resources. As an experienced provider of hosted services, ACI has proven procedures in place to efficiently manage the product deployment from initial implementation through ongoing support.

With the onsite delivery option, the ACI Online Banking Fraud Management solution software is installed on premise at the institution and managed by the customer. With this option, ACI Analytics fraud optimization processes are still managed by ACI staff through a secure network to the on-premise host. This delivery option gives the institution complete control of their software and network while leveraging the expertise of ACI in managing and optimizing fraud analytics and rules.

Summary

Enterprise Banker offers a full range of online banking capabilities with built-in security protocols including multifactor authentication, dual approval functions, browser security, velocity and limit threshold monitoring, and a full range of alerting and audit options. When implemented with Proactive Risk Manager, ACI's powerful fraud detection and prevention solution, end-users can be assured of a strong defense against risk and a complete approach for managing it in wholesale payments. ACI Online Banking Fraud Management offers a powerful, secure approach to monitoring login, ACH and wire activity initiated over the online banking channel, as part of a strong foundation to any online financial crime management strategy. In addition to reducing overall fraud, it also:

- **Provides brand value:** Publicized losses can damage an institution's credibility as a safe place to transact.
- **Lowers operational costs:** Targeted alerts for suspicious transactions require fewer operational resources; the intuitive interface improves average time per alert.
- **Increases deterrence:** Once criminals perceive an institution as difficult to breach, the number of fraud attempts can decrease significantly.
- **Bolsters confidence in the online banking channel:** New and emerging fraud trends threaten commercial customers' confidence of electronic payment channels.

→ ACI Online Banking Fraud Management is part of a strong foundation to any online financial crime management strategy.



ACI Professional Services

Whether implementing an ACI product for the first time or upgrading from an earlier version, ACI's professional services always provide the most cost-effective expertise. Backed by 35 years of experience and a strong commitment to customer satisfaction, ACI offers the highest levels of service in the industry.

Building on more than 2,000 successful software implementations worldwide, ACI has developed a comprehensive methodology for product delivery. The process will put a customer's new system into production and keep it operating at peak efficiency. Implementation services include project planning and management, installation and customer configuration to successfully integrate the solution into the customer's unique environment. Services also include custom software modifications if required, testing services and certification support, as well as go-live support.

Upgrading to new versions of ACI software is made easier by using ACI's technical consulting services. By taking care of everything from project management to retrofitting any existing customer-specific modifications to new product releases, ACI consultants help customers maintain their competitive edge and performance at peak efficiency.

Features at a glance

- Provides a single platform for online banking
- Supports multifactor authentication at logon, ACH release and wire release
- Sends alerts about key account events and activities
- Provides a detailed audit trail of all activities
- Offers multiple levels of approval for any online payment and administrative functions (new users, password changes, etc.)
- Delivers online banking ACH and wire fraud detection and prevention addressing
 - Account takeover
 - MITB (malware)
- Facilitates real-time monitoring of transactions, including approve, deny and refer options, and session login monitoring
- Offers an extensible platform for enterprise financial crime management
- Provides seamless interoperability between Enterprise Banker and Proactive Risk Manager
- Enables single vendor management for online banking fraud
- Recommends fraud prevention best practice rules and optimization for online banking
- Supports on-demand and onsite delivery options
- Delivers access to ACI financial crime management and payments experts
 - Online banking fraud operations review and recommendations
 - Rule testing and updating
- Provides a quick start implementation toolkit and documentation
 - Online banking fraud overview and how it happens
- Benefits from ACI industry leadership in payments and financial crime



ACI Worldwide

Offices in principal cities throughout the world
www.aciworldwide.com

Americas +1 402 390 7600

Asia Pacific +65 6334 4843

Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide 2011

All rights reserved. All product names are trademarks or registered trademarks of their respective companies. ACI and the ACI logo are trademarks or registered trademarks of ACI Worldwide or its subsidiaries in the United States, other countries or both.

ABR4558 02-11

About ACI Worldwide

ACI Worldwide powers electronic payments for financial institutions, retailers and processors around the world with the broadest, most integrated suite of electronic payment software in the market. More than 90 billion times each year, ACI's solutions process consumer payments. On an average day, ACI software manages more than US\$12 trillion in wholesale payments. And for more than 150 payments organizations worldwide, ACI software ensures people and businesses don't fall victim to financial crime. We are trusted globally based on our unrivaled understanding of payments and related processes. We have a definitive vision of how electronic payment systems will look in the future and we have the knowledge, scale and resources to deliver it. Since 1975, ACI has provided software solutions to the world's innovators. We welcome the opportunity to do the same for you.