

Securing the Online User Experience

Building User Confidence and Stopping Fraud

December 2007



Executive Summary

Every organization that provides individual service to its customers, employees, members, or community is faced with the very real concern of gaining and keeping their users' trust. Public awareness of phishing attacks, identity theft, and online fraud makes informed users wary of disclosing personal information without strong assurance that their data is safe and that the entities with which they interact are what they claim to be.

This benchmark report looks at those organizations that are getting the best results in both growing user confidence and reducing fraud. It examines the strategies, capabilities, and technology enablers that help these organizations get their notable results.

Research Benchmark

Aberdeen's Research Benchmarks provide an in-depth and comprehensive look into process, procedure, methodologies, and technologies with best practice identification and actionable recommendations

Best-in-Class Performance

Aberdeen used five key performance criteria to distinguish Best-in-Class companies. Over the last 12 months Best-in-Class companies:

- Increased the number of user accounts
- Increased number of online transactions
- Increased number of online transactions per user
- Reduced the number of incidents of fraud
- Reduced financial loss attributable to fraud

Competitive Maturity Assessment

Survey results show that the firms enjoying Best-in-Class performance shared several common characteristics:

- 92% authenticate users at the creation of the account
- 84% use encryption
- 68% monitor transactions

Required Actions

In addition to the specific recommendations in Chapter Three of this report, to achieve Best-in-Class performance, companies must be continuously educating themselves both on the new and different fraud threats, and on the new and emerging security enablers. Best-in-Class companies are getting tangibly better results than Industry Average and Laggard organizations, and across the board, they are adopting stronger security solutions.

Send to a Friend 

Table of Contents

Executive Summary.....	2
Best-in-Class Performance.....	2
Competitive Maturity Assessment.....	2
Required Actions.....	2
Chapter One: Benchmarking the Best-in-Class	4
Business Context	4
Competing Priorities	4
Shifting Sands	5
The Maturity Class Framework.....	6
The Best-in-Class PACE Model	7
Best-in-Class Strategies.....	8
Chapter Two: Benchmarking Requirements for Success	9
Competitive Assessment.....	9
Capabilities and Enablers.....	10
Chapter Three: Required Actions	13
Laggard Steps to Success.....	13
Industry Average Steps to Success	13
Best-in-Class Steps to Success.....	13
Appendix A: Research Methodology.....	15
Appendix B: Related Aberdeen Research.....	17

Figures

Figure 1: Leading Pressures Compelling Organizations to Focus on Securing the Online User Experience.....	5
Figure 2: Strategic Actions Driving Best-in-Class Investments in Securing the Online User Experience	6
Figure 3: caption	12

Tables

Table 1: Companies with Top Performance Earn Best-in-Class Status.....	7
Table 2: The Best-in-Class PACE Framework	7
Table 3: The Competitive Framework.....	10
Table 4: The PACE Framework Key	16
Table 5: The Competitive Framework Key	16
Table 6: The Relationship Between PACE and the Competitive Framework	16

Chapter One: Benchmarking the Best-in-Class

Business Context

Banks, e-tailers, utility companies, health-care providers, insurance companies, service providers, gaming providers, and all kinds of associations share a common problem: keeping the online experience of their customers or members safe and secure.

The economics of doing business online are compelling – reducing costs through self-service websites or portals, eliminating costly paper-based mailings, and 24 hour availability to name a few. (See Aberdeen's [Clicks to Customers](#), January 2007 benchmark report). But online fraud and identity theft continue to rise as customers continue to grow increasingly aware of the potential risks associated with disclosing personal data, which is having a dampening effect on their willingness to transact online. According to the Anti-Phishing Working Group, the number of unique phishing sites grew this August to 32,079. Current Aberdeen research indicates that concern over account holder confidence tops the list of pressures facing account providers.

For the purpose of this report, we refer to any organization that provisions a user account as an "account provider," and the end-user of that account as the "account holder." Examples of account providers and account holders include banks and their customers; utilities and their customers; universities and their students, faculty, and staff; gaming sites and their users; and non-profits and their members.

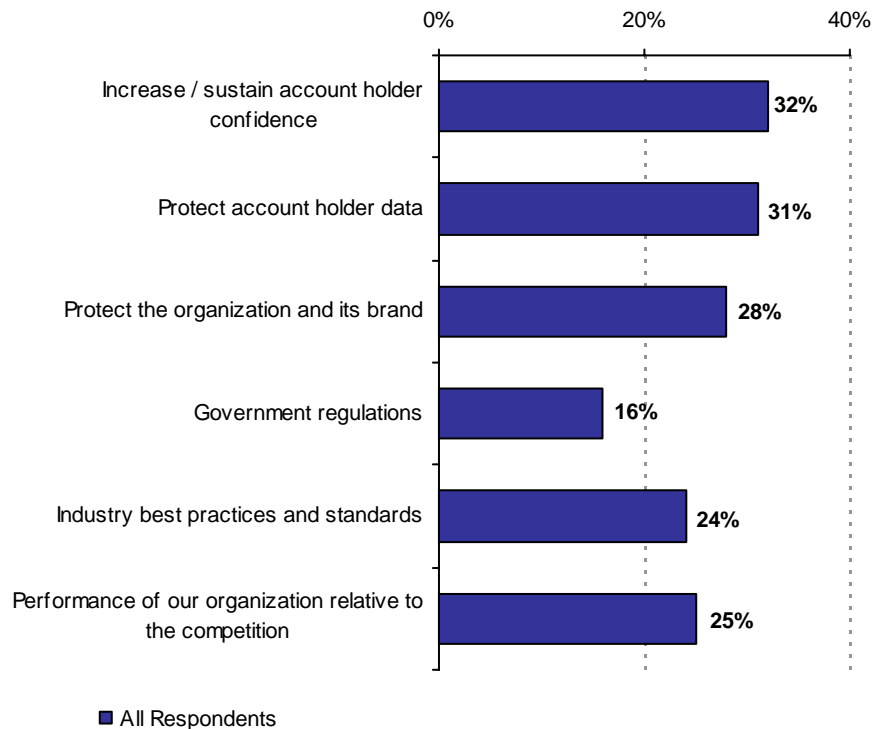
Competing Priorities

Account providers work to deter fraud to protect their own assets as well as those of their account holders. However, it is insufficient to address only the issue of fraud, because the results of fraud have eroded brands and consumer confidence. The problems of escalating fraud and increased consumer concern must be addressed in tandem because the level of consumer skepticism will not dissipate quickly even if fraud rates drop dramatically. Best-in-Class account providers understand that concurrent with directly confronting the ever-evolving fraud threats, they must also educate their account holders in safe online practice and inform them of the additional steps being taken to safeguard their data.

Fast Facts

- √ Best-in-Class are twice as likely as Industry Average and over three-times more likely than Laggard organizations to use risk-based authentication
- √ Best-in-Class are 50% more likely to use extended validation SSL certificates than Industry Average organizations

Figure 1: Leading Pressures Compelling Organizations to Focus on Securing the Online User Experience



Source: Aberdeen Group, December 2007

Shifting Sands

If we look at the adoption of online services across virtually every industry segment over the course of the last ten years, the direction is clear: online delivery of services is more cost-effective for the account providers, and potentially more convenient and cost-effective for their account holders.

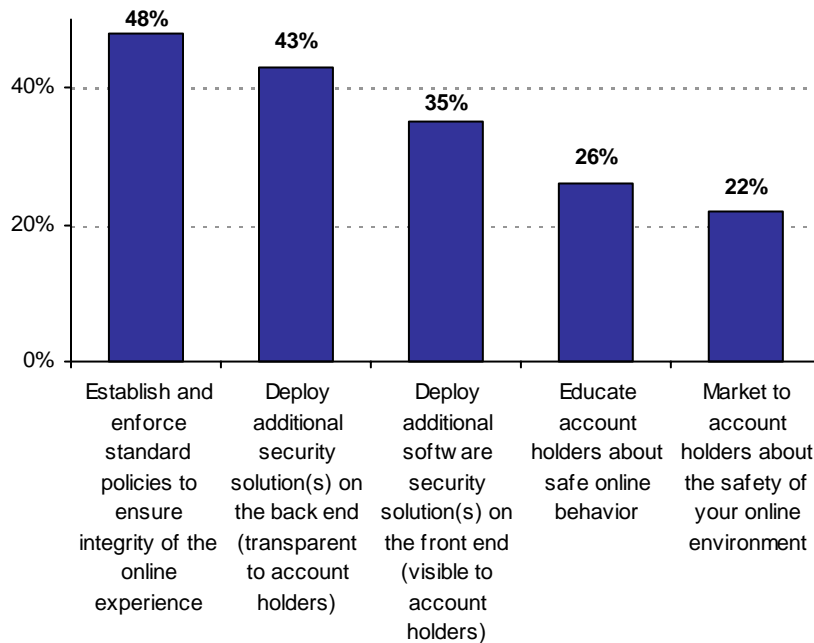
Driving account holders to use online services has shifted from carrots (e.g., providing incentives for adoption) to sticks (e.g., eliminating alternative channels or making them inconvenient or more expensive). For example, airline companies charge extra for using a reservation agent to book a ticket over the phone, and banks continue to close branch offices making banking in person less convenient.

In the drive toward adoption of online services, the mantra of "convenience to the user" rules - what is cumbersome for the account holders is typically ignored or circumvented. If sites are too difficult or too onerous to use, users find alternative sites or channels for their transactions - for example, they pick up the phone, or shop somewhere else. Under this dictum, the delicate balance between "user convenience" and "user security" has struggled.

Security perceived as too onerous is ignored - making something too difficult means that people simply won't do it. Thus, although many security

technologies that could conceivably be applied in an online services context have existed for a long time, when the choice of adoption has been put to the account holder, for the most part convenience has won out. Evidence is strong that adding more security to the back end (transparent to the account holder) is a top strategy for most organizations - 51% name it as one the top two strategic actions they employ (Figure 2).

Figure 2: Strategic Actions Driving Best-in-Class Investments in Securing the Online User Experience



Source: Aberdeen Group December 2007

Evidence suggests that in addition to deploying transparent / invisible security solutions, Best-in-Class account providers are beginning to deploy more visible (and sometimes ostensibly less-convenient) security technologies such as hardware tokens used to authenticate user accounts, increasingly in response to account holder demand. They also understand the need to simultaneously educate their account holders on safe practices and inform them of the initiatives in place to keep them safe.

The Maturity Class Framework

Aberdeen used five key performance criteria to distinguish the Best-in-Class companies from Industry Average and Laggard organizations in securing the online user experience. To measure account holder confidence focus was placed on the organization's ability to grow its account base, the number of transactions, and the number of transactions per user. To measure the organization's ability to stop fraud, we looked at the number of incidents of fraud and financial losses attributable to fraud. All measurements were over the past 12 months.

Table 1: Companies with Top Performance Earn Best-in-Class Status

Definition of Maturity Class	Mean Class Performance
Best-in-Class: Top 20% of aggregate performance scorers	<ul style="list-style-type: none"> ▪ 71% decreased the number of incidents of fraud ▪ 67% decreased financial loss attributable to fraud ▪ 100% increased the number of account holders ▪ 100% increased the number of online transactions ▪ 92% increased the number of transactions per account holder
Industry Average: Middle 50% of aggregate performance scorers	<ul style="list-style-type: none"> ▪ 29% decreased the number of incidents of fraud ▪ 29% decreased financial loss attributable to fraud ▪ 91% increased the number of account holders ▪ 86% increased the number of online transactions ▪ 54% increased the number of transactions per account holder
Laggard: Bottom 30% of aggregate performance scorers	<ul style="list-style-type: none"> ▪ 0% decreased the number of incidents of fraud ▪ 5% decreased financial loss attributable to fraud ▪ 16% increased the number of account holders ▪ 16% increased the number of online transactions ▪ 0% increased the number of transactions per account holder

“Our biggest concern with other organizations is not whether or not transmission encryption is employed but how do other organizations store their details. Having reviewed many online privacy policies, many mention SSL claiming their sites are secure. Yet they store data in their databases freetext without encryption. If their databases are stolen not only do they risk all data, consumers' behavior of re-using credentials (passwords, date of birth, mother's maiden name, etc.) are all subject to abuse.”

~ CEO, Australian Internet Hosting Company

Source: Aberdeen Group, December 2007

The Best-in-Class PACE Model

Securing the online user experience requires a combination of strategic actions, capabilities, and technology enablers. The nature of account holders, the frequency and value of transactions, and the data involved, vary from organization to organization, but the primary objectives in securing the online user experience are constant. Aberdeen's Pressures, Actions, Capabilities, and Enablers (PACE) Framework details the pressure most prevalent for the Best-in-Class organizations, their top strategic actions, the capabilities on which they rely, and the technology enablers they use to achieve their superior results.

Table 2: The Best-in-Class PACE Framework

Pressures	Actions	Capabilities	Enablers
<ul style="list-style-type: none"> ▪ Increase or sustain account holder confidence 	<ul style="list-style-type: none"> ▪ Establish and enforce standard policies to ensure the integrity of the online experience ▪ Deploy additional security solutions on the backend (transparent to the user) 	<ul style="list-style-type: none"> ▪ Match security solutions with the level of risk appropriate to each account holder segment ▪ Fraud detection with integrated threat analysis ▪ Anti-fraud directory ▪ Reward account holders for the adoption of visible security solutions such as site keys or authentication tokens ▪ Phone support for online transactions 	<ul style="list-style-type: none"> ▪ Initial authentication of account holders ▪ Smart cards ▪ Risk based authentication ▪ Hardware tokens ▪ Extended validation SSL server certificates ▪ Anti-phishing solution ▪ Transaction monitoring ▪ Data masking ▪ Electronic signature ▪ Shared anti-fraud network ▪ Transaction authorization

Source: Aberdeen Group, December 2007

Best-in-Class Strategies

Although the number one pressure cited by Best-in-Class organizations is to increase or sustain account holder confidence, close on its heels is to protect account holder data. Indeed these two strategies go hand in hand but require different initiatives and focus.

The top strategic action taken by the Best-in-Class is to establish and enforce standard policies to ensure the integrity of the online experience. This is different from the findings of all respondents which places deploying additional security on the backend (transparent to the user) as first. We think this noteworthy because we believe it reflects the Best-in-Class understanding of the necessity of the creation of and enforcement of standard policies which Aberdeen research has shown as critical to successful security initiatives throughout the whole of IT security.

Aberdeen Insights - Strategy

eBay, PayPal, Bank of America, and Wells Fargo were among the early victims of phishing attacks. As such, it's not surprising that these organizations have made concerted efforts to both persuade and protect their account holders. Wells took on a high-profile media campaign. Bank of America deployed site keys - perhaps more to bolster the appearance of protection than from actual protection of user accounts. eBay has an online tutorial on how to keep your account safe. PayPal has recently begun deploying physical security in the form of security keys - hardware tokens that can be used to protect both PayPal and eBay accounts.

Organizationally, new roles are emerging such as PayPal's Director of Account Protection and Verification.

Because of increased media attention to the risks of online transactions, the frequent reports of data breaches, and the increase in organization, sophistication, and volume of online fraud, account providers are finding that account holder confidence has been steadily declining. As the industry tries to keep up with creating more and better mechanisms for identifying and thwarting fraud, some users are becoming more ready to adopt technologies that in earlier years they eschewed. We attribute that readiness to several factors:

- The acceptance of the pervasive, ubiquitous single interface called the Internet
- The acknowledgement of the persistent, ever-evolving presence of maleficent forces such as fraud
- Increased user fluency with technology as generations growing up online mature and affirm the online space as integral to their lives

All these factors point to a demand for and insistence on a robust, secure online user experience.

In the next chapter, we look at what the top performers are doing to achieve these results.

“Because both eBay and PayPal customers have been the target of phishing attempts, we were looking for more ways to add security to their accounts,

The PayPal security key accomplishes this by adding an additional layer of security to their account. We are pleased with the adoption rate for the PayPal security key and have had a tremendously positive response to the device from our customers.

We believe that open standards are important. In beta testing the device, this was a concern we heard over and over again from our customers.

One significant advantage to the PayPal security key is its ability to be used on websites other than PayPal.”

~ Michael Vergara, Director of Account Protection and Verification, PayPal.

Chapter Two: Benchmarking Requirements for Success

Account holder confidence and preventing fraud go beyond protecting the business - they are integral to growing the communities they serve. For organizations conducting financial transactions online, increasing the number of customers or value of transactions of customers goes straight to the top line. For organizations tasked with serving their constituents online, reducing the costs associated with delivering service clearly impacts the bottom line.

Case Study - DebtHelp.com

Online debt consolidator DebtHelp.com was suffering serious brand erosion as the result of phishing attacks that diverted would-be prospects to fraudulent sites that captured and sold their credentials as leads to DebtHelp.com's competitors. "Confidence in online debt consolidation has been diminishing for the last seven years," says DebtHelp.com's President John Turner. "A lead in this area used to cost only about a dollar - now it's \$20 because of drastically reduced user confidence."

Seeking to combat the fraud and restore user confidence and brand, DebtHelp.com looked for innovative technology that might help. "I'm an early adopter" says Turner, "I'm always looking for new technologies that could make a difference." Turner found Extended Validation SSL certificates and was very excited by the idea but had no idea what effect they'd have on DebtHelp.com. DebtHelp.com was one of the first sites to adopt Extended Validation SSL certificates.

"I thought it'd be good, but I had no idea how effective it would be. We got an amazing increase in our form completion rate - up 11%. In the two years since we deployed Extended Validation SSL certificates we've realized an ROI of 16,000%! I never dreamed it would have this effect."

Fast Facts

- √ Best-in-Class organizations are more than twice as likely as Industry Average and more than three-times as likely as Laggard organizations to use an anti-fraud directory
- √ Best-in-Class organizations are more than 50% more likely to use electronic signatures than all organizations combined

Competitive Assessment

The aggregated performance of surveyed companies determined whether they ranked as Best-in-Class, Industry Average, or Laggard. In addition to having common performance levels, each class also shared characteristics in five key categories: (1) **process** (the ability to detect and respond to changing conditions without placing additional burdens on the organization); (2) **organization** (corporate focus and collaboration among stakeholders); (3) **knowledge management** (contextualizing data and exposing it to key stakeholders); (4) **technology** (the selection of appropriate tools and intelligent deployment of those tools); and (5) **performance management** (the ability of the organization to measure the benefits of technology deployment and use the results to improve key processes further). These characteristics (identified in Table 3) serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the key metrics.

Table 3: The Competitive Framework

	Best-in-Class	Average	Laggards
Process	Match security solutions with the level of risk appropriate to each account holder segment		
	57%	43%	34%
	Reward account holders for the adoption of visible security solutions such as site keys or authentication tokens		
	20%	14%	10%
	Phone support for online transactions		
	80%	65%	50%
	Online support (email) for online transactions		
	84%	73%	44%
Organization	Anti-fraud task force		
	42%	33%	30%
Knowledge	Real-time analysis and reporting		
	56%	39%	36%
	Anti-fraud directory		
	50%	32%	18%
Technology	Real time alerts		
	50%	39%	34%
	Fraud detection with integrated threat analysis		
	56%	32%	22%
Performance	Measures fraud		
	63%	31%	26%
	Measure account holder adoption of security mechanisms		
	38%	28%	16%

“We understand that our brand is associated with our online presence. Even though we outsource our bill-pay capability, we know that if anything goes awry, the customer will hold us accountable. We fully vet each of our vendors’ security capability before engaging with them.”

~Director, US Utility Company

Source: Aberdeen Group, December 2007

Capabilities and Enablers

Based on the findings of the Competitive Framework and interviews with end users, Aberdeen’s analysis of the Best-in-Class shows that in general, they are more attentive to and responsive to their account holders. Viewed across the dimensions of process, organization, knowledge, performance and technology integration, the Best-in-Class account-holders’ interests are well-represented.

Process

Whether measures such as providing phone and email support to account holders for online transactions by their simple availability lends credibility to

a site, or whether the help received interacting with the site helps account holders (or would-be account holders) overcome obstacles and objections and thereby gain confidence is hard to know. It may be that these investments made on the part of the account providers make for a useful barrier to entry to fraudsters.

Rewarding account holders for adopting security measures aids in the adoption of new technologies, but also boosts account holder confidence by virtue of the acknowledgement that something is actually being done to protect them and that they are an active part of the process.

The cost of security ought always to be measured against the actual potential loss. Best-in-Class companies understand that different customer segments represent different levels of risk, and allocate more resources to protect greater risk.

Organization

Organizations that take fraud seriously are creating working groups to address the on-going, ever-changing nature of the threats that fraud represents. Inherent in this formation is the understanding that although fraud has always existed, the global nature of online transactions and the well-organized and well-funded stature that fraud has attained mean that ongoing vigilance and inventiveness are required to keep pace.

Knowledge Management

A significant advancement in thwarting fraud is being made by trying to identify the fraud while it's taking place rather than after it's happened. To this end, organizations are using varied technologies to provide data for real-time analysis and reporting. Organizations that use real-time reporting and analysis and avail themselves of the use of an anti-fraud directory are getting better results than those that don't.

Technology

The shift in fraud prevention is toward the identification of fraud in the moment - the ability to stop fraud in real-time. To the arsenal of fraud defense include adding more layers of user authentication, geo-location, and device authentication. As fraud becomes more sophisticated so must the defense. The more data that can be brought to bear without creating false positives that result in lost business, the better. Organizations must not only protect their own account holders but also guard against the use of synthetic identities - identities created from pieces of legitimate criteria cobbled together for the express purpose of committing fraud. Best-in-Class account providers are nearly 50% more likely to use real-time reporting of fraud than the Industry Average, 33% more likely to use geo-location services, and 20% more likely to use device authentication - all technologies aimed at stopping fraud in action.

Performance Management

Organizations need to find tangible metrics to assess their own capabilities and liabilities with regard to secure online user experience. Beginning by

"I'm worried about online commerce. I've seen large banks use self-signed digital certificates. That's the same as me presenting a drivers license I made with PhotoShop. I really don't think people understand the seriousness of the threats to e-commerce. I believe many organizations think that there is so much money to be made so easily by doing e-commerce, that the pressures to get things online push security to the back. They say, "When we have a chance, we will go back and do security," and it never really gets done right or at all since they've got to release the next rev soon."

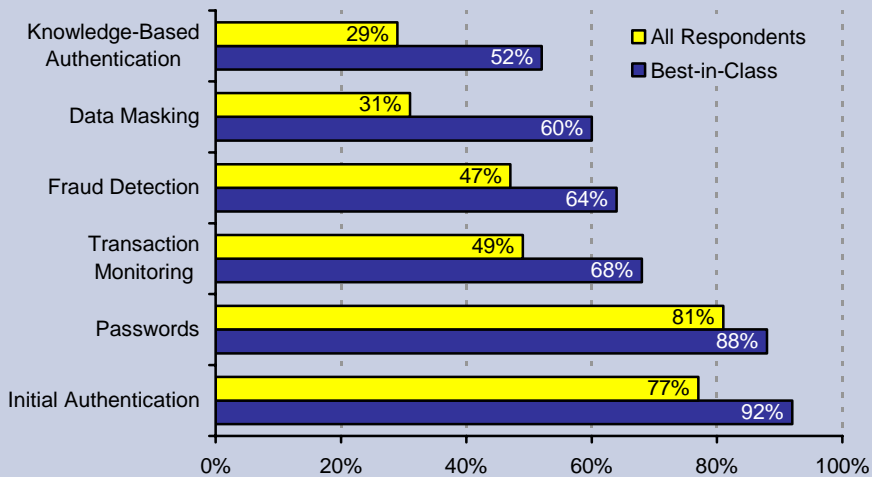
~ IT Security Manager,
Human Capital Consulting
Firm

measuring fraud and account holder behaviors gives visibility into both pillars of secure online user experience.

Aberdeen Insights - Technology

Best-in-Class organizations out pace all respondents in technology adoption to stop fraud.

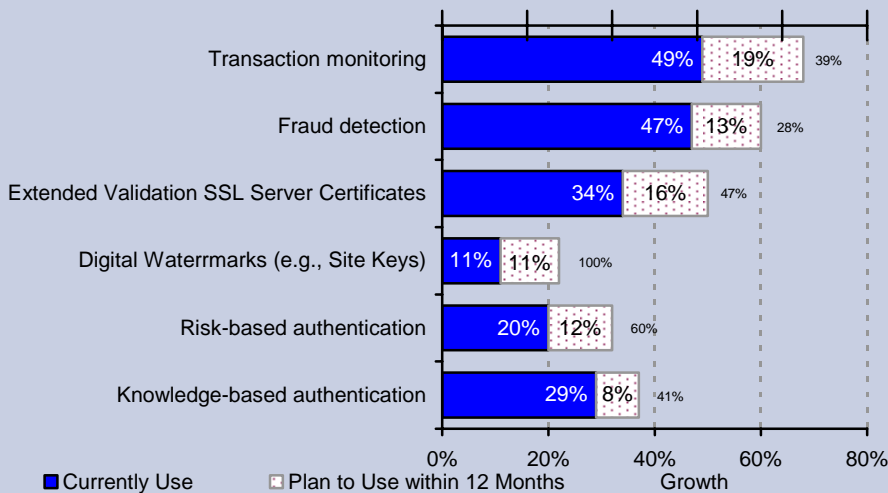
Figure 3: Select Technology Enablers used by Best-in-Class



Source: Aberdeen Group, December 2007

No single anti-fraud deterrent is sufficient. As account providers shore up their defenses, those that do not will more readily become prey to the automated attacks constantly searching for vulnerable sites to exploit.

Figure 4: Current and Planned Use – Select Enabling Technologies



Source: Aberdeen Group, December 2007

Chapter Three: Required Actions

Whether a company is trying to move its performance in securing the online user experience from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help spur the necessary performance improvements:

Laggard Steps to Success

- The first step Laggard organizations must take is to implement initial authentication of account holders by deploying an authentication solution. Compared to the Best-in-Class, 92% of which use initial authentication, only 58% of Laggard organizations do.
- Implement data masking. Only 14% of Laggard organizations use data masking compared with 60% of the Best-in-Class. Chances are these organizations are not compliant with the Payment Card Industry (PCI) Data Security Standard, but even for organizations that do not use credit card information, patient identifiable information, social security numbers, and other sensitive information must be protected.
- Provide support for online transactions. Only 44% of Laggard organizations provide online support via email versus 84% of Best-in-Class companies. Helping account holders through transactions helps boost confidence and complete transactions.

Industry Average Steps to Success

- Measure the number of incidents of fraud and the financial loss associated with each incident. Measure how many user accounts are active, how many transactions each generates, and the value of those transactions.
- Provide phone support for online transactions. Only 65% of Industry Average organizations provide phone support compared with 80% of the Best-in-Class. Investing in phone support can help bolster account holder confidence and help deter fraud.
- Use an automated anti-fraud directory to eliminate transactions with entities already identified as fraudulent by other account providers.

Best-in-Class Steps to Success

- Continue the movement toward more real-time fraud analysis and the integration of elements such as geo-location and device authentication.
- Provide account holders with choices of additional security including hardware tokens, where appropriate. For those account holders

Fast Facts

- ✓ Best-in-Class companies are nearly twice as likely to use data masking than all respondents
- ✓ Best-in-class are 38% more likely to use phone authentication than all respondents

"We're very concerned about the increase in online fraud. We do over a billion dollars in online ecommerce annually. We're looking at two-factor authentication. PCI has greatly increased online security. It will be much better when people really implement all of PCI 1.1, including web application pen tests and DB protection."

~Architect, Global Hotel Chain

comfortable with using, taking care of, and keeping track of hardware tokens, they're a good option. Others find this kind of solution cumbersome or intimidating. It's important to offer solutions appropriate to the expectations and competencies of the account holder.

- Reward account holders for the adoption of stronger security mechanisms. This makes the transactions safer and actively engages account holders in the protection of their account contributing to account holder confidence.

Aberdeen Insights - Summary

Across the board, the account providers we talked to are all concerned about rising online fraud and the future of ecommerce. None is sitting comfortably by content that they are forever secure. Knowing that the future will demand even more security, creating policies to manage security consistently should be high priority for all account providers.

Best-in-Class companies teach us that consistent policy is core to their success. What can be done transparently (invisible to the account holder) should be done invisibly. Tolerance for stronger authentication varies from account holder to account holder. Make stronger authentication choices such as hardware tokens, available but not mandatory, allowing account holders to adopt to their own degree of tolerance.

The contention between user convenience and strong security is a false dichotomy - it's perfectly possible to have both, and more importantly, strong security that's not easy to use won't be used.

The increased sophistication and determination of contemporary fraudsters continue to up the ante with insidious, pernicious attacks that keep account providers on the defense. As organized criminal gangs create synthetic identities, spoof location and perpetrate massive automated attacks, account providers must be diligent in providing the best security possible, and the best security possible is a moving target. Yesterday's protection is simply not enough.

Send to a Friend 

Appendix A: Research Methodology

In November 2007, Aberdeen examined the use, the experiences, and the intentions of more than 100 organizations with the mandate of securing the user experience of their account holders.

Aberdeen supplemented this online survey effort with email and telephone interviews with many survey respondents, gathering additional information on their strategies, experiences, and results.

Responding enterprises included the following:

- **Job title/function:** The research sample included respondents with the following job titles: C-level executive (CEO, COO, CIO, CFO, President) 24%; vice president / director (18%); and manager or staff (35%).
- **Industry:** The research sample included respondents exclusively from these industries: finance / banking / accounting was the largest segment with 29% of the sample. High technology/ software for 19% of respondents, retail (8%), and telecommunications services (6%).
- **Geography:** The majority of respondents (60%) were from North America. Remaining respondents were from the Asia-Pacific region (15%), and Europe (25%).
- **Company size:** 40% of respondents were from large enterprises (headcount over 2,500); 23% were from midsize enterprises (headcount between 100 and 2,500); and 37% of respondents were from small businesses (head count of 100 or less).

Solution providers recognized as sponsors of this report were solicited after the fact and had no substantive influence on the direction of the *Securing the Online User Experience* benchmark report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge.

Study Focus

Responding executives completed an online survey that included questions designed to determine the following:

- √ The degree to which they are effectively reducing fraud
- √ The degree of account holder confidence
- √ Key strategies in gaining user confidence and stopping fraud
- √ The use of technology enablers in stopping fraud and gaining user confidence

The study aimed to identify emerging best practices for securing online user experience, and to provide a framework by which readers could assess their own capabilities

Table 4: The PACE Framework Key

Overview
<p>Aberdeen applies a methodology to benchmark research that evaluates the business pressures, actions, capabilities, and enablers (PACE) that indicate corporate behavior in specific business processes. These terms are defined as follows:</p> <p>Pressures — external forces that impact an organization’s market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, competitive)</p> <p>Actions — the strategic approaches that an organization takes in response to industry pressures (e.g., align the corporate business model to leverage industry opportunities, such as product / service strategy, target markets, financial strategy, go-to-market, and sales strategy)</p> <p>Capabilities — the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing)</p> <p>Enablers — the key functionality of technology solutions required to support the organization’s enabling business practices (e.g., development platform, applications, network connectivity, user interface, training and support, partner interfaces, data cleansing, and management)</p>

Source: Aberdeen Group, December 2007

Table 5: The Competitive Framework Key

Overview	
<p>The Aberdeen Competitive Framework defines enterprises as falling into one of the following three levels of practices and performance:</p> <p>Best-in-Class (20%) — Practices that are the best currently being employed and are significantly superior to the Industry Average, and result in the top industry performance.</p> <p>Industry Average (50%) — Practices that represent the average or norm, and result in average industry performance.</p> <p>Laggards (30%) — Practices that are significantly behind the average of the industry, and result in below average performance.</p>	<p>In the following categories:</p> <p>Process — What is the scope of process standardization? What is the efficiency and effectiveness of this process?</p> <p>Organization — How is your company currently organized to manage and optimize this particular process?</p> <p>Knowledge — What visibility do you have into key data and intelligence required to manage this process?</p> <p>Technology — What level of automation have you used to support this process? How is this automation integrated and aligned?</p> <p>Performance — What do you measure? How frequently? What’s your actual performance?</p>

Source: Aberdeen Group, December 2007

Table 6: The Relationship Between PACE and the Competitive Framework

PACE and the Competitive Framework – How They Interact
<p>Aberdeen research indicates that companies that identify the most impactful pressures and take the most transformational and effective actions are most likely to achieve superior performance. The level of competitive performance that a company achieves is strongly determined by the PACE choices that they make and how well they execute those decisions.</p>

Source: Aberdeen Group, December 2007

Appendix B: Related Aberdeen Research

Related Aberdeen research that forms a companion or reference to this report includes:

- [Thwarting Data Loss – Best-in-Class Strategies for Protecting Sensitive Data](#) – May 2007
- [Ins and Outs of Email Vulnerability](#); July 2007
- [Who's Got the NAC? Best Practices in Protecting Network Access](#) October 2007
- [Sustaining Compliance](#); September 2007
- [Encryption & Key Management](#); August 2007
- [Aligning IT with the Business](#); June 2007
- [Protecting Cardholder Data: Best-in-Class Performance at Addressing the PCI Data Security Standard](#); June 2007
- [Clicks to Customers](#), January 2007

Information on these and any other Aberdeen publications can be found at www.Aberdeen.com.

Author: Carol Baroudi, Research Director, IT Security,
carol.baroudi@aberdeen.com

Founded in 1988, Aberdeen Group is the technology- driven research destination of choice for the global business executive. Aberdeen Group has 400,000 research members in over 36 countries around the world that both participate in and direct the most comprehensive technology-driven value chain research in the market. Through its continued fact-based research, benchmarking, and actionable analysis, Aberdeen Group offers global business and technology executives a unique mix of actionable research, KPIs, tools, and services. This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provides for objective fact based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen's analytical and independent view of the "customer optimization" process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen <http://www.aberdeen.com> or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to <http://www.harte-hanks.com>