

January 12, 2005

Keeping Financial Transactions Online

by Jonathan Penn and Penny Gillespie

BEST PRACTICES

BEST PRACTICES

Client Choice topic

January 12, 2005

Keeping Financial Transactions Online

Stronger And More Visible Security Will Attract Customers

by **Jonathan Penn and Penny Gillespie**

with Bill Doyle and Adele Sage

EXECUTIVE SUMMARY

Fraud and identity theft continue to rise, making consumers and small business owners more concerned and skeptical about online security and data privacy. If financial organizations want to continue their online momentum, then they must redefine the balance between security and customer convenience. Smart firms will be more overt in demonstrating stronger security and promoting this as an element of customer advocacy.

TABLE OF CONTENTS

2 **Customers' Security Concerns Threaten Online Finance**

Firms Underestimate The True Cost Of The Problem

Online Channel Use Suffers

Customers View Firms As Unresponsive To Their Security Needs

6 **Rebuilding Trust: Security As An Element Of Customer Advocacy**

Why Trust Matters

How Firms Are Starting To Rebuild Trust

Where Firms Need To Go

RECOMMENDATIONS

9 **Market Security As An Element Of Customer Advocacy**

WHAT IT MEANS

10 **New Business Opportunities For Early Adopters**

NOTES & RESOURCES

Forrester discussed this topic with dozens of security and business executives at leading financial firms and with many security vendors focused on fighting fraud and identity theft.

Related Research Documents

"Why Small Business Customers Don't Bank Online"

December 10, 2004, Trends

"Phishing Concerns Impact Consumer Online Financial Behavior"

December 2, 2004, Trends

"Combating Fraud In Financial Services"

April 7, 2004, Best Practices

CUSTOMERS' SECURITY CONCERNS THREATEN ONLINE FINANCE

Customer data has become extremely valuable because criminals can use the data to access the supporting financial assets and to create new credit accounts. As incentives have risen, criminals have become more technically savvy in committing fraud and identity theft, using approaches like phishing and key logging.

As fraud and identity theft increase, so too does customer awareness of these threats. As a result, consumers are losing trust in the online financial channel at a time when adoption is beginning to grow quickly. The evidence clearly indicates that this erosion of trust is impeding the adoption of online financial transactions. Because the cyber threats will only get worse, the continuation of this trend seriously jeopardizes the long-term viability of online financial transactions.

Firms Underestimate The True Cost Of The Problem

Many firms assess the impact of fraud and identity theft in terms of direct losses, which can be quite hefty. Take credit card number compromises, for example. In addition to the liability for losses, the card-issuing bank also has the expense of canceling existing cards and issuing new ones. But spikes in customer support calls and increased spend on security and marketing to respond to security incidents drive up firms' costs.

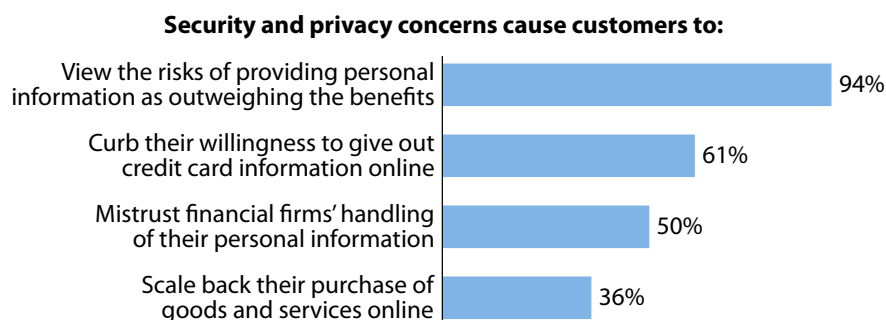
These indirect costs, however, provide the greatest cause for concern and present the most compelling justification for firms to take significant action. Firms that don't improve security will find that:

- **Online finance adoption slows.** Concerns over privacy and security of personal information are a major reason why people don't enroll or stop using online banking and bill pay services.
- **eMarketing loses its effectiveness.** With the rise in spoofed messages and phishing attacks, consumers are less inclined to open email purported to be from their own financial provider.
- **Right-channeling doesn't happen.** Customers who might have used the online channel don't and instead continue to turn to the branch and the call center for assistance. As a result, support costs don't come down.

Online Channel Use Suffers

Consumers are becoming wary of using online channels to provide credit card numbers and personal information. In fact, 50% actually mistrust their financial firm's handling of their personal information (see Figure 1). And nearly 30% of respondents to an American Banker survey conducted this past year said that they think a bank has violated their financial privacy.¹

The statistics show that these behavioral changes are most pronounced among the type of customers that financial firms most want to target.

Figure 1 Safety Concerns Shape Consumer Perceptions Of The Internet

Base: US households

Source: Forrester's Consumer Technographics® 2003-2004 North American Benchmark Studies

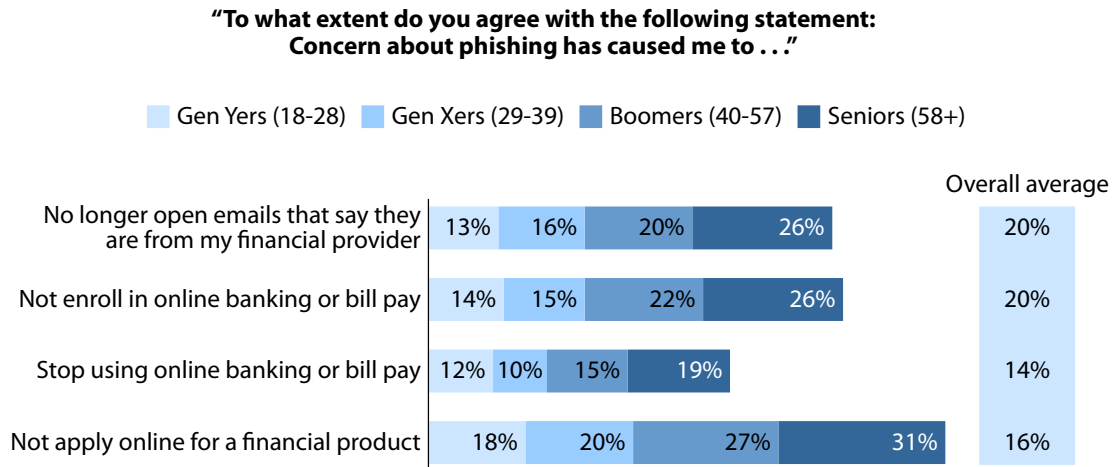
Source: Forrester Research, Inc.

- **Impact increases with age.** The curbing of online financial activity due to security concerns increases with age (see Figure 2). It is also observed more with women than with men. And while three-fourths of all online consumers are concerned about email fraud, Boomers were the group most likely to express this concern.
- **The affluent small business owner is most wary.** Nineteen percent of affluent small business owners declined to apply for a credit product online because of concerns about security and data privacy (see Figure 3-1). Small business owners are also changing their behavior when it comes to activities like emailing, banking online, and applying for financial services products online (see Figure 3-2).
- **Identity theft victims hold back from online activity.** Victims of identity theft are more concerned than others about online theft and fraud, and they curb their behaviors more than others due to privacy concerns. Yet these victims tend to have higher incomes and more online experience. They are also more likely to engage online if their privacy concerns are addressed.²

Customers View Firms As Unresponsive To Their Security Needs

Although they may not always articulate it well, customers want and need more security to foster trustworthiness. Even 15 months ago when Forrester first broached the topic in market surveys, consumers and small business owners most frequently cited their concern about the privacy and security of their data as a reason for not banking online. Assumptions made several years ago about how much security is enough and which inconveniences users would accept in the name of security and privacy no longer apply.

Figure 2 Privacy And Security Concerns Affect The Behavior Of Key Customers



Base: US online consumers who answered “agree” or “strongly agree”

Source: Forrester’s Consumer Technographics® August 2004 North American Finance Online Study

Source: Forrester Research, Inc.

Customers want to know that their data is safeguarded. Yet, a small business banking survey this past year indicated that only 56% of the participating banks were offering customized and tiered access, and only 22% were offering digital certificates to their small business banking customers.³

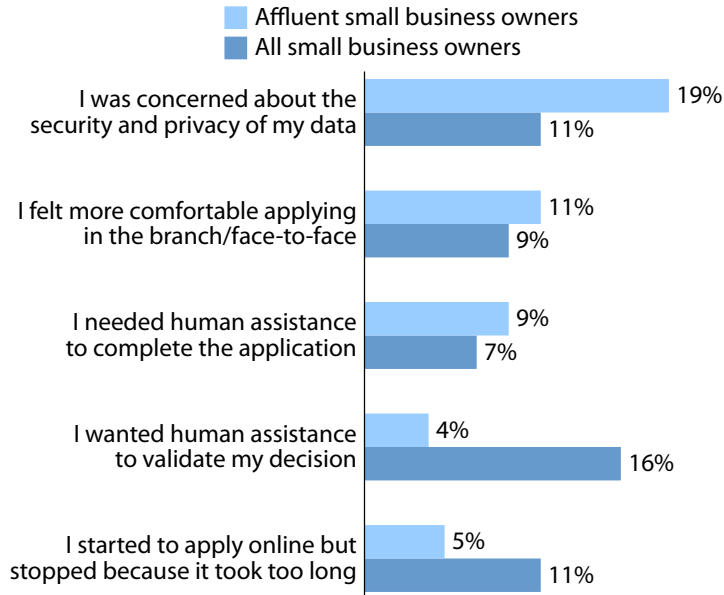
Worse yet, some firms actually *enable* fraud by sending unsolicited email messages asking for personal information, failing to sufficiently authenticate customers, and having undisciplined and lax procedures for data access. In many cases, financial firms use multiple domain names, which add to the confusion. Occasionally, credit card data has even been accessible through search engines like Google.

The good news: Many consumers and small business owners are willing to add extra steps in return for more secure transactions. For example, consumers say they are willing to type in a password or additional numbers when entering their credit card number (see Figure 4). Among small business owners, there is pent-up demand for tiered access, an indication that the group is looking for better security for financial transactions.⁴

Figure 3 Security And Privacy Concerns Affect Small Businesses

3-1 Security and privacy concerns deter small business owners from applying for online credit products

“Why didn’t you apply for credit products online?”

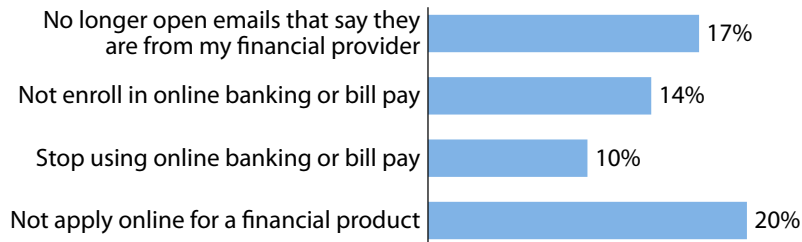


Base: US consumers who have applied for credit products

Source: Forrester’s Consumer Technographics® Q3 2003 North American Study and Forrester’s Consumer Technographics® Q3 2003 North American Affluent Mail Study

3-2 Security concerns cause some small business owners to change their online behavior

**“To what extent do you agree with the following statement:
Concern about phishing has caused me to . . .”**

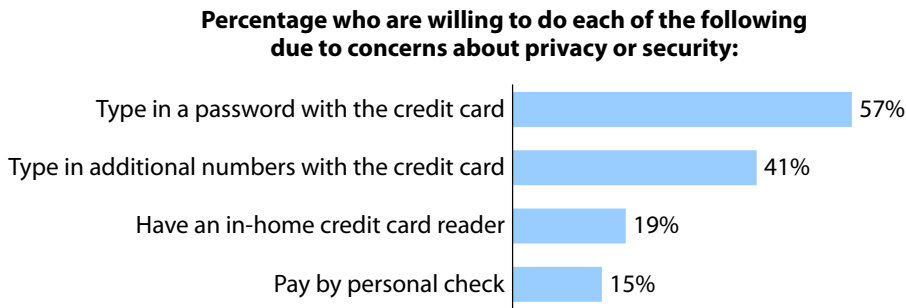


Base: US online consumers who are small business owners and who answered “agree” or “strongly agree”

Source: Forrester’s Consumer Technographics® August 2004 North American Finance Online Study

Source: Forrester Research, Inc.

Figure 4 Consumers Are Willing To Take Measures For Increased Security



Base: US online households

Source: Forrester’s Consumer Technographics® Q4 2003 North American Study

Source: Forrester Research, Inc.

REBUILDING TRUST: SECURITY AS AN ELEMENT OF CUSTOMER ADVOCACY

Financial firms need to re-establish lost trust when it comes to data security and privacy. Trust goes beyond the security measures themselves; it encompasses customer awareness and understanding of the measures. It includes not just what a firm would do to protect the customer, but also what it would do to make the customer whole in the event of a breach. Thus, firms must communicate better about security activities and privacy policies and put stronger security guarantees in place to improve customer perceptions of trustworthiness.

Why Trust Matters

Trust is a key ingredient to high-value relationships between customers and the businesses with which they engage online. Trustworthiness translates into doing what’s right for the customer — whether the activity is regulated or not. It means that a financial institution honors its promises and goes out of its way to protect privacy. It is one of four key components of customer advocacy: the perception on the part of the customers that the firm has their best interests at heart, not just the firm’s own bottom line.⁵ Financial firms viewed as strong customer advocates are those mostly likely to generate higher satisfaction, greater cross-sell potential, and deeper relationships with their customers. Customers who consider their financial firm to be a customer advocate are more likely to have a broader relationship with the firm, encompassing banking and investments.

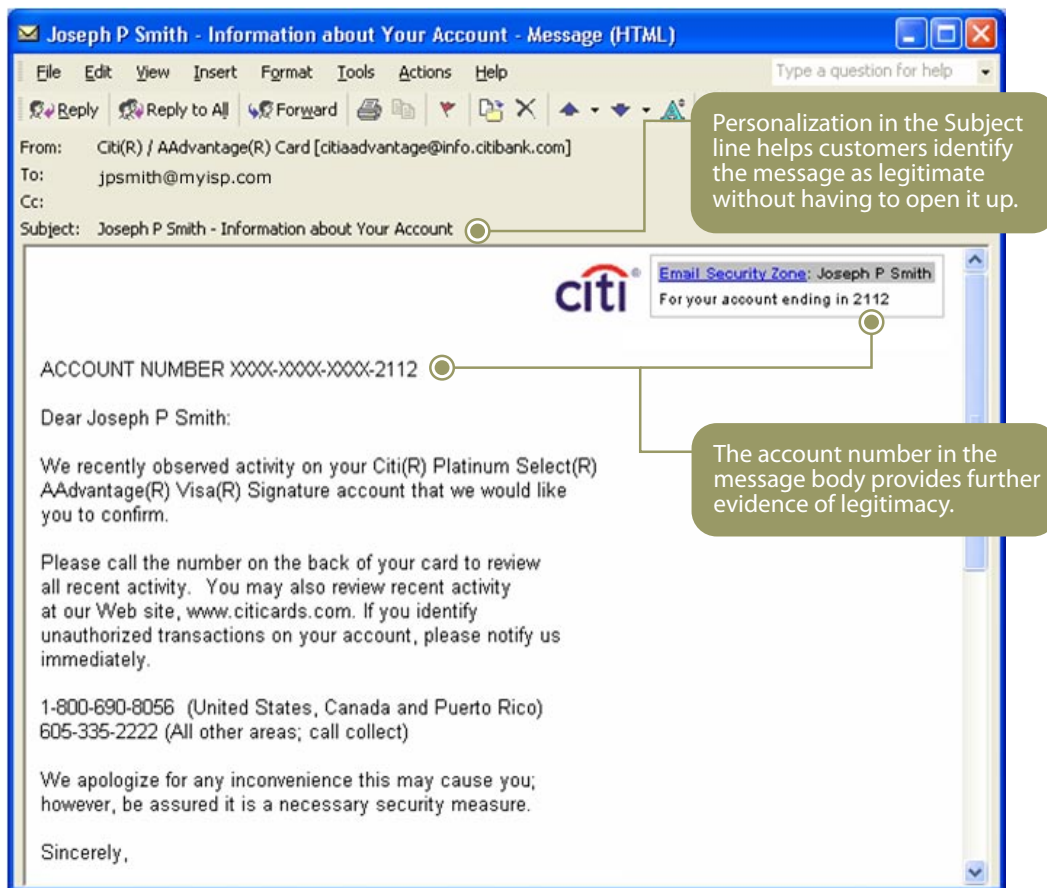
Firms responsive to changing market demands will strengthen their security measures — even at the expense of customer convenience — to demonstrate a clear commitment to customer advocacy. Customers need to understand how stronger security can make identity theft and fraud more difficult to commit, how the firm is willing to assist them when potential problems are identified, and how both visible and unseen protections are safeguarding their information and their privacy.

How Firms Are Starting To Rebuild Trust

Savvy financial firms are starting to get it and are moving to reassure their customers. These firms not only recognize their customers' concerns but are also demonstrating that they are serving customers' best interests through education, additional protection services, and guarantees. Here are examples of good practices from financial leaders:

- **Citi email offers assurance of validity.** Recently, Citi added more personalization to customer email messages and now includes and highlights the last four digits of the customer's account number (see Figure 5). With these simple methods, Citi enables customers to validate message legitimacy for themselves. While this approach doesn't detect forgeries, it reassures the customer both to the legitimacy of the specific message and that Citi is aware of and responding to customer concerns over email fraud.

Figure 5 Citi Mechanisms Allow Customers To Identify Legitimate Email



Source: Citi

Source: Forrester Research, Inc.

- **Wells Fargo goes the extra mile in response to a security breach.** When a computer with Wells Fargo customer data was stolen from one of the consulting firms it uses, the bank was compelled to notify California residents per that state's privacy law CA SB-1386. Wells contacted all customers — not just Californians — both by mail and phone. It didn't just notify them to the possible misuse of their personal data, but it also provided customers with advice on how to monitor their credit ratings. Going even further, Wells Fargo offered to pay for a year's worth of service from a third-party credit-monitoring company.

Although some may view this event as causing erosion of trust because personal information might have been compromised, it is an excellent example of how to respond to security breaches that could compromise customer data. Wells did what was best for the customer — exhibiting a lesson learned from the Tylenol scare experienced by Johnson & Johnson — thus averting a potential catastrophe.⁶

- **Bank of America offers an explicit guarantee.** Bank of America offers “zero liability” for customers of its credit cards, check cards, and home equity line of access cards. As part of this free service, the bank promises next-day reimbursement of losses from stolen credit cards and unauthorized purchases that are promptly reported to the bank.
- **PNC and Washington Mutual offer free ID-theft insurance.** PNC began offering coverage to customers with multiple accounts, covering expenses associated with restoring a credit history. Washington Mutual offers its coverage to its checking account customers, which includes up to \$5,000 for recovery expenses. It covers all accounts and banking relationships held by the customer.
- **Royal Bank of Canada and Standard Bank of South Africa secure customer PCs.** These banks distribute personal firewall software to its online banking customers to help prevent intrusion and the stealing of key bank data, such as user IDs and passwords.

Where Firms Need To Go

Although the steps being taken by financial firm leaders are a step in the right direction, they are not sufficient. The balance between convenience and security has changed. Consumers want more protection and are willing to take additional steps for their personal security and data privacy. More drastic changes are needed. Many solutions only report fraud and do not prevent it, especially for high-profile online account hijacking and identity theft.

Firms need a two-front attack: improved customer authentication and greater controls over processes and policies. Furthermore, both of these need to be well conveyed to customers as elements of customer advocacy and looking out for customers' best interest.

- **Strong authentication protects accounts even when passwords are compromised.** The only true cure for the most visible fraudulent activities today is two-factor authentication. By implementing two-factor authentication, such as a PIN token, a smart card calculator, or some other mechanism to generate one-time codes, passwords would have no value to hackers. Phishing and key logging would cease because there would be no benefit from it.
- **Business controls prevent data theft.** Insider attack is still the largest source of data for identity theft and fraud. Financial firms should limit employee access to customer data. They should also protect and limit the amount of sensitive customer data stored on PCs, which can be stolen easily. Social security numbers cannot be used as key data fields. Financial firms must also make partners follow the same prescription for data access and use appropriate procedures and due diligence when giving third parties access to data.

RECOMMENDATIONS

MARKET SECURITY AS AN ELEMENT OF CUSTOMER ADVOCACY

It's time to take security out of the closet. Firms must advertise their advocacy of customer security in ways that communicate trustworthiness. It doesn't work anymore to avoid talking about security and consumer protections. People are scared, and they show it by curbing their online financial activity. But better security alone is insufficient; customers require more visible assurances that their accounts and data are protected. Successful firms will market security as an element of customer advocacy — looking out for the customer's best interest — and implement it in ways more visible to the customer. Ultimately, customers view an organization's security and privacy protections — or lack thereof — as an important factor in determining the trustworthiness of doing business with it.⁷

How exactly can firms incorporate security into customer advocacy? Here are five tips:

- **Communicate what you're doing.** Competing firms will start to position themselves based on security and privacy protections. You may be doing a good job, but if customers don't know it, they'll start moving elsewhere.
- **Provide customers with identity theft protection and guarantees.** Firms should offer free credit reporting services to valued customers. Identity theft victims should be guaranteed timely remuneration and free credit recovery services.
- **Go above and beyond legislative requirements.** Customers are demanding greater protections in response to sophisticated criminal activity. In the fast-paced world of hacking tool kits and hit-and-run scams, laws move too slowly.
- **Start moving to two-factor authentication.** It's simple: The only way to fully protect against online account thieves who steal customers' passwords is to require more than just

passwords for online access. Firms should begin exploring solution options, integration strategies, and customer adoption campaigns.

- **Foot the bill.** Firms can't get away with charging extra for security. Customers expect their financial providers to be good custodians of their data. Ever-changing security demands are part of the cost of doing business.

WHAT IT MEANS

NEW BUSINESS OPPORTUNITIES FOR EARLY ADOPTERS

Security and privacy concerns are driving financial customers to view protection as a significant factor when choosing their provider and determining how much business to do with it. The convenience of online banking is just starting to be recognized, and when bundled under stronger security and as a fraud-monitoring tool, both consumers and small business customers will come forward. Financial firms that are quick to increase security and position this as customer advocacy will take market share away from other financial firms.

ENDNOTES

- ¹ This perception is even greater in certain types of households — those with annual household incomes greater than \$75,000 and those located in the West and Northeast. Source: American Banker/Gallup Consumer Survey, conducted by telephone April 5 through May 7, 2004. The Gallup Organization contacted 1,000 heads of households in the US using random digit dialing. All participants had some type of financial account (depository, loan, or credit card) with a financial institution. Statistical margin of error is plus or minus 3% at a 95% confidence level on questions answered by all respondents.
- ² A surprising 9% of US online customers have experienced identity theft. See the June 21, 2004, Trends “Consumer Concerns Over Identity Theft And Fraud.”
- ³ We surveyed 55 banks during Q2 2004 to identify their online small business product offerings. We asked the banks about their current offerings and planned offerings. An additional 20% reported plans to implement customized and tiered access in the next 12 months, whereas only 9% reported plans to implement digital certificates in the next 12 months.
- ⁴ We surveyed 55 banks and numerous consumers. For the most part, customers were unaware of bank offerings, which had a direct impact on their usage. Tiered access, however, was more widely used among the small population that was aware of it, suggesting pent-up demand for it. See the December 10, 2004, Trends “Why Small Business Customers Don't Bank Online.”
- ⁵ The four elements of customer advocacy are simplicity, trust, benevolence, and transparency. See the June 2, 2004, Trends “What Satisfies Financial Services Consumers.”

- ⁶ Johnson & Johnson is often cited as one of the best examples of crisis management. In 1982, its Tylenol product was compromised, forcing prompt action. The company immediately went public with the compromise and addressed customer issues, which allowed it to maintain its market share.
- ⁷ Trustworthiness is a key component of customer advocacy, and the financial firms viewed as strong customer advocates were those mostly likely to have higher satisfaction, greater cross-sell potential, and deeper relationships with its customers. See the June 2, 2004, Trends “What Satisfies Financial Services Consumers.”

FORRESTER®

Helping Business Thrive On Technology Change

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617/613-6000
Fax: +1 617/613-5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia	Japan
Brazil	Korea
Canada	The Netherlands
France	Sweden
Germany	Switzerland
Hong Kong	United Kingdom
India	United States
Israel	

*For a complete list of worldwide locations,
visit www.forrester.com/about.*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866/367-7378, +1 617/617-5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.