The True Cost of Protecting Customers' Online Accounts

...is it a cost at all?

18 AUGUST 2005
QUANTITATIVE RESEARCH REPORT
RSA SECURITY INC.

RSA SECURITY

Overview

Contents

- What prompted RSA Security to undertake this research?
- What were the study's objectives & methodology?
- How did consumers respond to hardware-based strong authentication?
- How can hardware-based strong authentication help account providers?
- Research conclusions

Objectives of the research

- Determine how the current environment is impacting consumer perceptions and behaviors
- Determine if consumers would be willing to adopt device-based strong authentication
- Understand if and how device-based account protection impacts consumers attitudes and behaviors
- Quantify the value consumers place in this form of online account protection

Research methodology

- Online survey among 8,198 online users actively engaged in online account-based activities
- Administered by LightSpeed Research to its panel participants between May 10 – May 18
- Targeting four distinct audiences: online traders, online auction participants, online bankers, and web portal/mail users (~ 2,000 per group)

RSA SECURITY

What prompted RSA Security to undertake this research?

The current environment

As consumers rely upon the Internet for more and more of their daily activity, they face growing concerns over information security. Almost exclusively, consumer account security is provided via single-factor authentication, i.e., account user name and password. However, the recent rash of identity-related transgressions by some businesses, a notable increase in the number and frequency of phishing attacks, and the proliferation of keylogging spyware have all served to heighten consumer sensitivity to online account fraud. Media coverage of such threats has shifted consumers' perceptions, eroding confidence in transacting online. In fact, a recent Informa Research study found that consumer confidence in transacting online – which had been on the rise from 2000 to 2003 – dipped sharply in 2005 from 70% to 59%.

Media coverage of identity-related transgressions intensifies

- Lost and stolen data have made **identity theft top-of-mind** for consumers:
  - Choice Point
  - Wachovia
  - Citibank
  - DSW
  - MasterCard
  - Time Warner
  - Bank of America
  - Commerce Bancorp
  - And more…

…Meanwhile, phishing attacks proliferate

- 2,870 active phishing sites were reported in March 2005 alone—an **increase of 28% per month**[1]
- According to a leading industry analyst, nearly **1 million U.S. consumers were defrauded** through phishing between May 2003 – 2004

[1] Anti-Phishing Working Group, 2005.

The impact on consumer perceptions

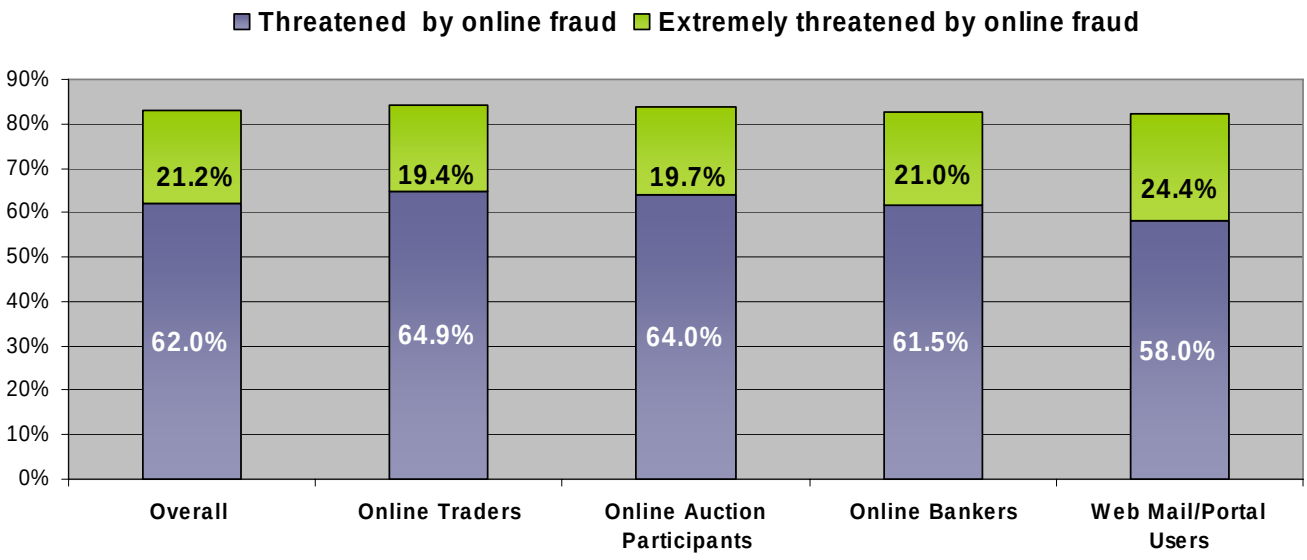
The current environment, cont'd

To better understand the current consumer environment, RSA Security undertook a quantitative study of 8,200 online consumers in the United States in May 2005. This research showed that over one-fifth of all online consumers feel *extremely* threatened by online fraud, and that two-thirds are concerned that someone will fraudulently access specific online accounts.

Impacting consumers' perceptions of their online security

Q: "How threatened do you feel by online fraud?"

A: One-fifth of all consumers felt extremely threatened



RSA SECURITY

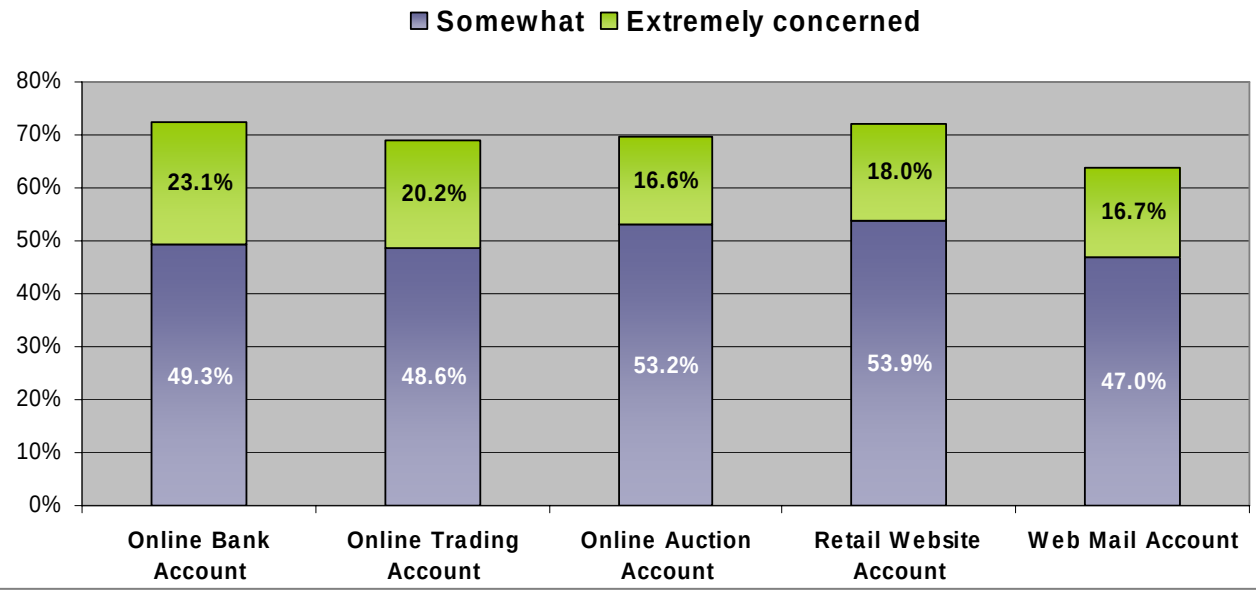
The impact on consumer perceptions

Anxiety about unauthorized access to specific accounts...

This general concern about online fraud translates into pointed concern around the protection of online accounts that relate to financial management or transactions. When asked about specific online accounts, two thirds of all consumers felt concerned about unauthorized access to common account-types.

Q: "How concerned are you that someone will fraudulently access your online _____ account?"

A: Two-thirds of all consumers felt concerned



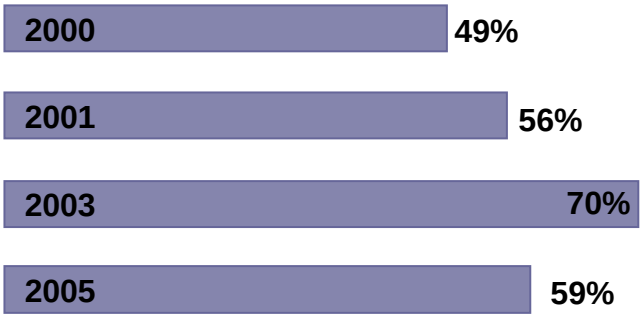
RSA SECURITY

The toll on consumer behavior

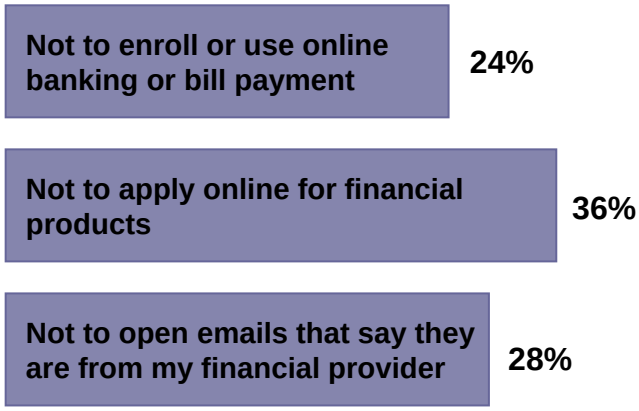
Third-party research indicates that this decline in consumer confidence is taking a toll on consumers' willingness to transact online. Concerns about email fraud impact online consumers' financial behavior. Twenty-six percent of online consumers report that phishing concerns have caused them not to apply online for a financial product. And 14% of online consumers have stopped using online banking and bill pay due to email fraud concerns.

Lack of confidence in transacting online

Consumer confidence, which had been on the rise from 2000 to 2003, has moved sharply lower[1]…



Of online consumers, online fraud concerns have convinced[2]…



But is two-factor authentication the solution?...

RSA SECURITY

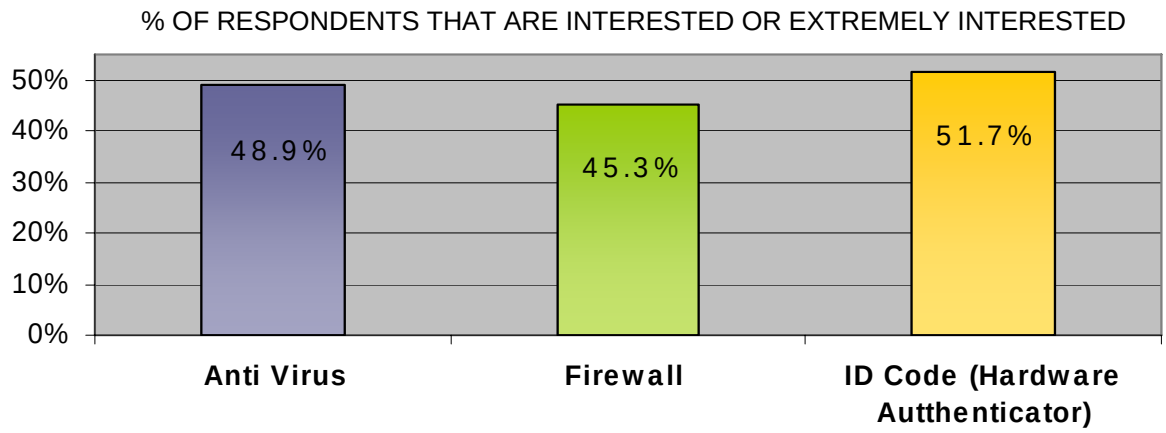
[1] Informa Research Services, August 2005.
[2] *Phishing Concerns Impact Consumer Online Financial Behavior*, Forrester Research, Inc., *December 2004.*

Do consumers see value in device-based strong authentication?

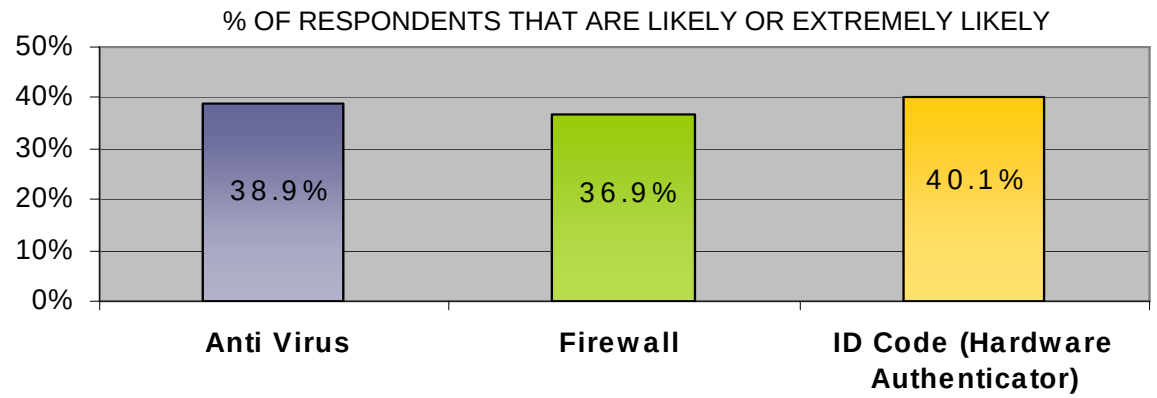
Can device-based strong authentication help?

We exposed consumers to the concept of device-based strong authentication to answer this critical question – and to gauge their interest in, willingness to adopt and willingness to pay for such a service. Included in the concept-testing were two widely-adopted consumer online security solutions – a firewall offering and an anti-virus service – to serve as benchmarks in the study. Including these gave us reference points to measure how well consumers were responding to the Hardware Authenticator concept. The research demonstrated that consumers are *not only* interested in the hardware authenticator solution, they are willing to adopt it – 40% of respondents were likely or extremely likely to adopt this form of account protection.

Q: "How interested are you in this service?"



Q: "How likely are you to adopt a service such as this service?"



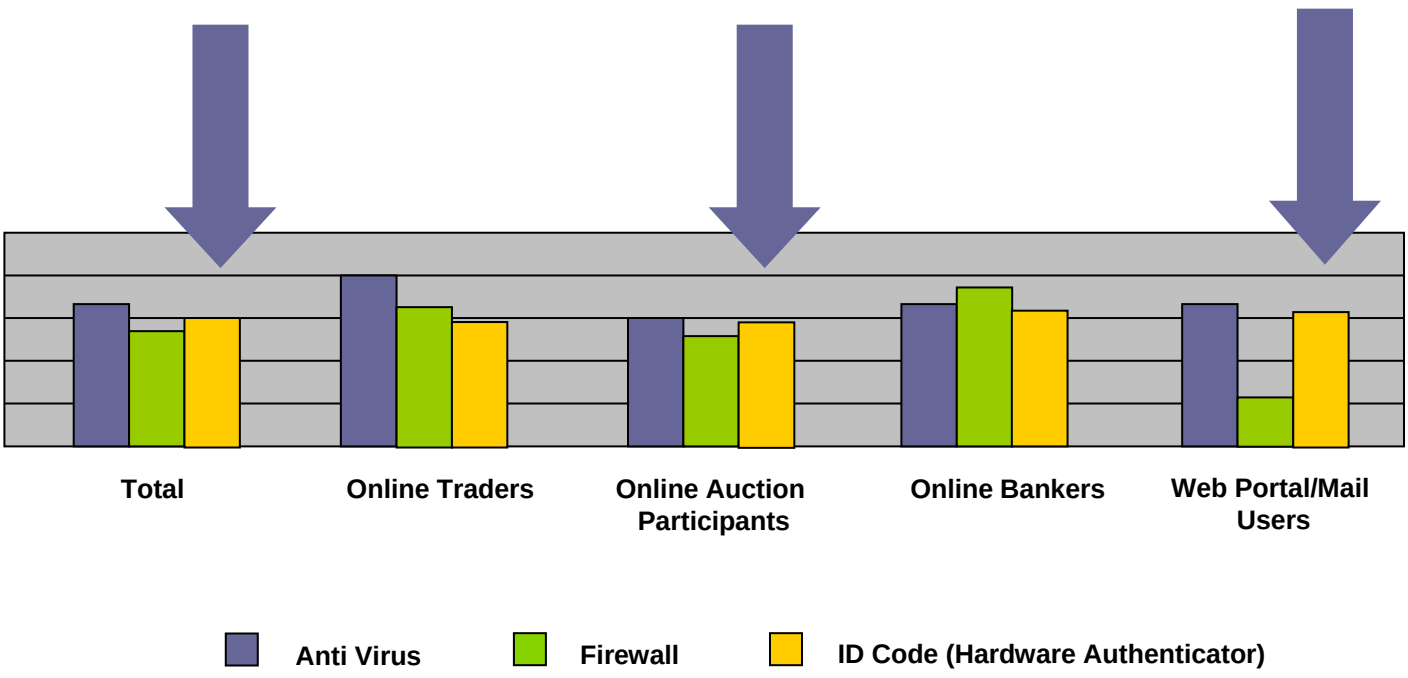
RSA SECURITY

Do consumers see value in device-based strong authentication?

Can device-based strong authentication help, cont'd...

Furthermore, a sizeable portion of the respondents said they would pay for the solution when tested at price points that mirror online security product norms. This percentage was on par with the proportion of respondents that would be extremely likely to subscribe to such mainstream and widely-adopted online security services as anti-virus and firewall. The research showed that a hardware authenticator achieved purchase intent scores at the same level as a firewall and only slightly lower than that of an anti-virus offering. Notably, the study revealed a greater purchase intent for a Hardware Authenticator than for a firewall at the same price point among key audiences.

INDEX OF TOP-BOX PURCHASE INTENT (EXTREMELY LIKELY TO SUBSCRIBE)



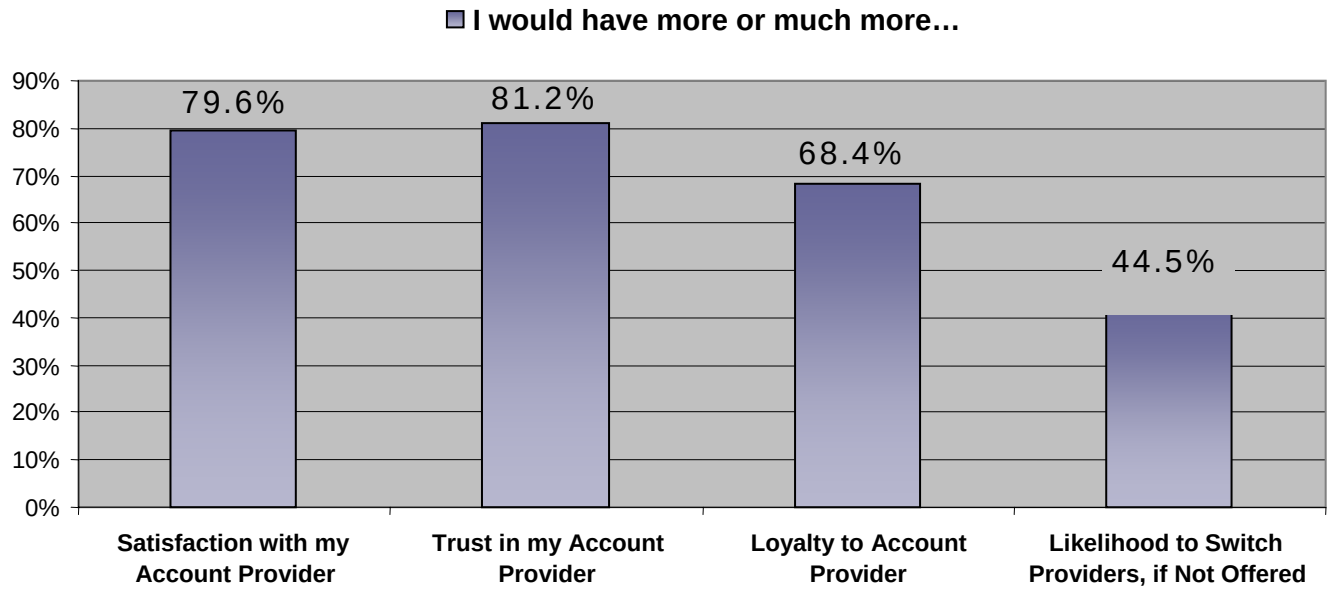
NOTE: Firewall and ID Code were tested at exactly the same price point. Anti Virus was tested a 25% lower price point based on market pricing norms.

Can strong authentication help to reverse the trend?

But can strong authentication help to address consumers' concerns?

The research demonstrated that offering strong authentication can impact consumer attitudes and behaviors. Eighty percent of survey respondents said it would increase their satisfaction with – and trust in – their account provider. Sixty-eight percent said it would increase their loyalty to their account provider. Heightened satisfaction increases the likelihood a customer will expand the amount of business they conduct with a particular account provider, and the ability to retain valuable customers leads to less marketing dollars being spent to acquire new clients. Conversely, when asked if their current account provider did not offer a service such as this, but a competitive provider did (holding all other services equal), nearly 45% said they would be more or MUCH more likely to switch providers. This suggests that hardware-based strong authentication can not only act as a retention tool, but that it could equally serve as a point of differentiation and an acquisition tool.

Q: "If your account provider were to offer a service such as this, how would it impact your _____?"



RSA SECURITY

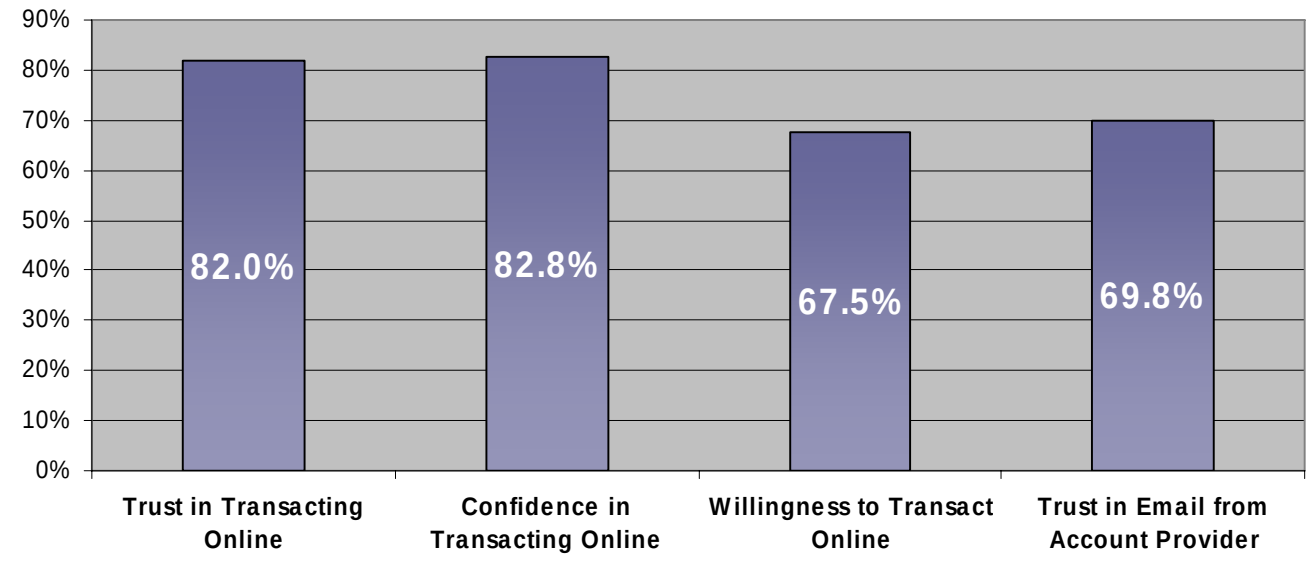
Can strong authentication help to reverse the trend?

But can strong authentication help to address consumers' concerns, cont'd...

Finally, 82% of consumers said hardware-based strong authentication would increase their trust and confidence in transacting online, with 67% saying they would be more willing to move more transactions online from offline channels. Likewise, it would increase the consumers' trust in email from an account provider.

By empowering consumers to conduct more of their transactions online versus offline, and encouraging them to receive important relationship-building communications via email instead of snail-mail, hardware-based strong authentication can reduce a company's overall transaction costs – in addition to serving as a retention and acquisition tool.

Q: "If your account provider were to offer a service such as this, how would it impact your _____?"



RSA SECURITY

Conclusions

Offering hardware-based strong authentication…

- Builds consumer **TRUST** and **CONFIDENCE** in transacting online
- Increases **SATISFACTION** with and **LOYALTY** to their account provider
- Can **IMPACT CONSUMERS' CHOICE** of account providers
- Engenders a greater **WILLINGNESS TO TRANSACT** online
- Creates a willingness to **MOVE TRANSACTIONS ONLINE** from offline

- AND, a sizeable number of consumers are **WILLING TO PAY** for this account protection

Hardware-based strong authentication has the potential not to be a cost driver at all. It has the potential to pay for itself many times over through reduced transaction costs, a greater share of the customer base and increased customer retention. Hardware-based strong authentication can even open up a new, incremental revenue stream for forward-thinking companies: consumers are *willing to pay* for security services that they deem valuable – and will even appreciate their account providers for offering such a service.