IdenTrust™

# Identity Management: Are You Willing to Risk Your Reputation On It?


All You Need is One.

*Enabling an eco-friendly digital world.*

**White Paper**

## ABOUT THIS WHITE PAPER

Financial institutions are in the business of managing risk and as a result bankers are used to mitigating credit, market, legal, operational and liquidity risks using complex, numeric, structures and discrete and clear models. Bankers have typically paid less attention to reputational risk, but this type of risk has always been as important. In addition, like other types of risk, reputational risk also has elements that can be modeled and analyzed.

Reputations can be damaged by unsavory business practices, discriminatory hiring, and executive indiscretion. However, reputations can also be destroyed by security breaches that weaken customers' trust in their financial institution.

This white paper looks at the impact of reputational risk as it pertains to security breaches from phishing and pharming attacks as well as non-compliance with regulations, and offers financial institutions a secure method of protecting its most valuable asset: its reputation as a safe and trustworthy institution.

## TABLE OF CONTENTS

## THE VALUE OF REPUTATION

What is reputation? According the American Heritage Dictionary, reputation is: 1. The general estimation in which a person [or business] is held by the public. 2. The state or situation of being held in high esteem. 3. A specific characteristic or trait ascribed to a person or thing: *a reputation for courtesy*.

A damaged reputation can cost an organization in terms of decreased brand value; lowered share price; lost customers, partners and strategic relationships; and difficulty recruiting and keeping top-notch employees. Simply put, losing your reputation translates into huge economic losses. Recovery can take years; some reputations never recover.

In a Financial Times article titled *The Challenge of Protecting Reputation*, Professor Paul A. Argenti of the Tuck School of Business at Dartmouth College asks, "Why is it so easy for executives to think about and plan for financial risks, but still so hard for them to understand that intangible risks to an organization's reputation are far more likely to destroy shareholder value?"

Reputation is all about perception. A reputation is tenuous. Reputation is also thought to be difficult to quantify.

However, organizations that have seen their good reputations dissolve may be able to put a value on reputation: priceless.

As reported on the Federal Trade Commission (FTC) web site, there were 130 major U.S. security breaches in 2005 representing $55 million in loses. Unfortunately, that $55 million is simply the tip of the proverbial iceberg. The following are just a few examples of organizations that have suffered large financial losses as a result of tarnished reputations:

- Arthur Andersen will never recover from its ruined reputation as the accounting firm involved in the Enron scandal. Says Time magazine in its January 17, 2002 issue, "Arthur Andersen's reputation as an honest accountant is now permanently tarred, and it will suffer at Wall Street's hands for devaluing its auditor's seal of approval."

- Its stature and reputation as Britain's oldest merchant bank and the Queen's personal bank was not enough to save Barings Brothers Bank. Nick Leeson, a rogue trader in Singapore, single-handedly brought down the firm and 230 years of banking history with it. ING acquired its debt and purchased Barings for a measly £1.

- A series of news reports about its accounting and business methods severely damaged the reputation of American International Group (AIG). Reports CBS MarketWatch on July 8, 2005, "AIG, one of the largest insurers in the world, has been rocked this year by multiple investigations into its accounting. The company's shares are down more than 16 percent since it disclosed inquiries by Attorney General Elliot Spitzer and the Securities and Exchange Commission on Feb. 14."

- Following news that identity thieves had gained access to personal consumer information, ChoicePoint, Inc.'s market cap dropped by $720 million. As a result of the security breach, the provider of identification and credential verification services has to pay a $10 million federal fine, contribute $5 million to a fund to compensate consumers who suffered from the breach and submit to external security audits for 20 years. Analyst estimates are that the security breach will cost ChoicePoint upwards of $30 million.

> *"Why is it so easy for executives to think about and plan for financial risks, but still so hard for them to understand that intangible risks to an organization's reputation are far more likely to destroy shareholder value?"*
>
> — Professor Paul A. Argenti
> Tuck School of Business,
> Dartmouth College

> *"Defend your reputation, or bid farewell to your good life for ever."*
>
> — William Shakespeare

- The Bank of Credit and Commerce International, or BCCI, earned a reputation as a rogue bank with dealings in money laundering and drug trafficking, to name a few. These suspicions forced the Bank of England to finally shut it down in 1991.

- CardSystems Solutions, Inc. was a billion dollar company before its security breach that compromised 40 million consumer accounts. After the breach, the company was acquired by Pay By Touch™ Payment Solutions, LLC. for a fire sale price of $47 million.

## The Value of Reputation in Financial Services

> *It used to take years of dedicated bad management to destroy a company. Now it can be done almost overnight.*
>
> — Sir John Bond, Former Chairman, HSBC

While reputation is important for all organizations, it is especially critical for financial institutions. Financial institutions rely on customer trust. Customers use banks because they trust them to take care of their money. If you lose trust, what do you have? Why would anyone put their money in a bank? Why not just put it under a mattress?

However, many financial institutions, especially smaller banks, are not protecting against reputational risk because they cannot quantify or measure the risk. Instead, they focus on risks they are comfortable with and that are more readily quantifiable and easier to protect against--market risk, credit risk, liquidity risk, and regulatory risk, to name a few.

Increased phishing and pharming attacks and the fear that banks are not secure are already having an impact on customers and the way they interact with financial institutions, according to research firm Gartner. For example, online banking customers are changing their usage patterns including logging in less frequently and no longer using online bill payment services.

Says Avivah Litan, Vice President and Research Director at Gartner, "Companies need to take steps quickly to beef up online security. Businesses cannot rely on the Internet to lower costs and improve marketing efforts indefinitely if consumer trust continues to decline."

Financial institutions are specifically at risk, says Litan. "This figure [indicating changing usage patterns] has serious implications for banks and other companies that want to use the e-mail channel to communicate more cost-effectively with their customer base. For example, a bill sent electronically costs about half of what a bill costs when sent through the regular mail."

> *I trust that bank. That is why I am keeping my money there.*
>
> — Trust and Loyalty in Client-Bank Relationships, Harvard University

The media has focused on the problem of identity theft and the protection of consumer information, even to the point of being confrontational toward financial institutions. Headlines like the following don't help the reputation of financial institutions: "*Banks Hang Fraud Victims High and Dry*" from MoneyCentral.msn.com. The Sun newspaper reported that it was able to purchase personal information including addresses, passwords, credit card details and passport information on 1,000 account holders of major UK retail banks from a call center agent in India. According to newspaper accounts, the reporter was also promised access to information about 1,000 additional bank customers every month.

*We know that trust has a value. Ask any Arthur Andersen Partner and they will tell you how much trust is worth to them.*

— The Agile Business Coach

## ONE CHANCE, MAYBE TWO...

So just how tenuous is a financial institution's reputation? According to the Ponemon Institute's 2006 *Privacy Trust Study for Retail Banking*, banks are only one or two security breaches away from losing their customers. While 68 percent of customers give their bank high marks for protecting their personal information, those customers report that only two security breaches would destroy that trust. Thirty-four percent of respondents would transfer their funds after a single security breach; 45 percent after two security breaches.

Once trust is lost, consumers will transfer their accounts to a different financial institution. Fifty-eight percent of those consumers surveyed said that a security breach would decrease their sense of trust and confidence in the organization reporting the incident. Only 8 percent of respondents did not blame the organization that reported the breach. Surprisingly, 12 percent said the incident enhanced their sense of confidence in the organization.

And if you think the answer to mitigating reputational risk is to keep mum on minor security breaches, think again. According to the Ponemon Institute, more than 82 percent of consumers believe that an organization should always report a breach, even if the lost or stolen data was encrypted or there was no criminal intent.

## REPUTATION KEEPS BANKERS UP AT NIGHT

*"Financial institutions are increasingly attuned to the dangers posed by less quantifiable risk but they need to turn their good intentions into action. Less quantifiable forms of risk can do as much, if not more, damage to companies' reputations, shareholder value and the long-term sustainability of their business as the more straightforward types of risk," says Phil Rivett, Global Leader of the Banking/Capital Markets Group at PricewaterhouseCoopers.*

The good news is that financial services executives are beginning to take notice of the impact of reputational risk. According to the 2004 PricewaterhouseCoopers study *Managing Risk: An Assessment of CEO Preparedness*, financial services executives now regard reputational risk as the greatest threat to an organization's market value. According to the study, 28 percent of financial services bosses felt that reputational risk was a significant threat and 13 percent felt it was one of the biggest threats they face.

*Glass, china, and reputation are easily cracked, and never mended well.*

— Benjamin Franklin

When asked which was a larger threat to their financial institution: known risks such as credit risk or unknown risks including reputational risk, 57 percent were most concerned about unknown risks.

*Which areas of risk represent the greatest potential threat to your organization's market value and earnings? (% of respondents rating as top area of focus; rank in brackets)*

| | **Market Value** | **Earnings** |
|---|---|---|
| Reputational risk | 34% (1) | 22% (6) |
| Credit risk | 25% (2) | 37% (1) |
| Market risk | 25% (3) | 31% (2) |
| Regulatory risk | 18% (4) | 25% (3) |
| Business/strategic risk | 16% (5) | 23% (4 tie) |
| Operational risk | 14% (6) | 23% (4 tie) |
| Business continuity risk | 13% (7 tie) | 13% (8 tie) |
| IT/technology risk | 13% (7 tie) | 8% (10 tie) |
| Treasury/liquidity planning | 10% (9) | 19% (6) |
| Governance risk | 7% (10 tie) | 13% (8 tie) |
| Sovereign/political risk | 7% (10 tie) | 8% (10 tie) |

*Source: PricewaterhouseCoopers/Economist Intelligence Unit survey, June-July 2004*

*"Our assets are our people, capital, and reputation. If any of these is ever diminished, the last is the most difficult to restore."*

— Goldman Sachs
Business Principles

## PLOTing AN EXCELLENT REPUTATION

If a financial institution is only one or two security breaches—no matter how inconsequential those breaches may be—away from having its reputation tarnished and having customers lose trust in the institutions' ability to keep their data and money safe, the question that should keep financial services executives up at night should be "How can I protect my financial institution from a security breach?"

It is becoming more evident that simple technology, even with stronger levels such as two-factor authentication, does not provide the level of protection needed to safeguard consumer and financial institution data. As recent events, such as the well-publicized man-in-the-middle attack against a large global bank demonstrate, criminals have found ways to circumvent two-factor authentication.

There is only one surefire way to secure customer and financial institution data and protect your financial institution's reputation: a secured proprietary network similar to those in place at Visa, MasterCard, and SWIFT—all of which have not suffered a security breach and continue to uphold their reputations as secure networks.

Like the networks powering Visa, MasterCard, and SWIFT, the IdenTrust network is made up of members. Because access is restricted to members who agree to common policies, guidelines and a legal framework for handling identities—unlike the very public Internet—IdenTrust can provide 100 percent assurance against security breaches, including insidious man-in-the-middle attacks that result from hackers inserting themselves between the originator and the end source. IdenTrust also delivers the benefits of using open published technology standards and applications once inside the network. Thus, IdenTrust provides the protection of a proprietary network with the flexibility of open, standards-based application provides.

Although the word "proprietary" has gotten a bad rap in a world increasingly enamored (and rightfully so) of open networks, software, operating systems and the like, it's the proprietary nature of the IdenTrust network that provides 100 percent certainty that your reputation will remain intact. Relying on the public Internet for hosting digital certificates is not secure. As financial institutions are painfully discovering, man-in-the-middle attacks are possible, and will no doubt increase in frequency.

As a members-only network, financial institutions around the world have agreed on a set of policies (P), legal framework (L), operations (O) and technology (T). PLOT provides the rules to transact business between customers of a single bank, between customers of multiple banks and between banks themselves for authenticating, validating, storing and encrypting identities and then relying on those identities as they were vetted by each other.

## CONCLUSION

Mitigating against reputational risk has never been more important due to the increase in phishing and pharming attacks and identity fraud. Although bankers may be most comfortable analyzing risks such as credit and market risk, they need to turn their attention to protecting their reputations since a damaged reputation can translate into huge monetary losses and a ruined perception in the marketplace that is difficult, if not impossible, to recover from.

The solution that can best protect financial institutions from any type of security breach and in turn protect their reputations is to become a member of a secure, proprietary network architected to protect its member institutions, such as IdenTrust.

> *"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."*
>
> — Warren Buffett

## ABOUT IDENTRUST

IdenTrust is the global leader in trusted identity solutions, recognized by global financial institutions, government agencies and departments, and commercial organizations around the world. IdenTrust enables organizations to effectively manage the risks associated with identity authentication; work interoperably with countries around the world; minimize investment in creating their own policies and legal frameworks; and deploy a spectrum of products insuring trust, smarter, faster, and more cost effectively.

The only bank-developed identity authentication system, IdenTrust provides a unique legally and technologically interoperable environment for authenticating and using identities worldwide. The IdenTrust Trust Infrastructure is predicated on a proprietary framework that combines policies, legal framework, trusted operations and technology (P.L.O.T.) to create a comprehensive environment for issuing trusted identities. IdenTrust is the only company to provide a solution incorporating all four of these elements. Customer agreements are valid, binding and enforceable in more than 175 countries. IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Competing offerings, in contrast, rely on a dizzying maze of public laws that vary from jurisdiction to jurisdiction. Additionally, the IdenTrust Trust Infrastructure maintains the privacy of each and every transaction processed by reading only digital certificate information, not the message itself.

Additional information can be found at www.IdenTrust.com.

**Corporate Headquarters**
IdenTrust Inc.
55 Hawthorne Street, Suite 400
San Francisco, CA 94105
USA
Telephone: +1.866.IDENTRUST (+1.866.433.6878)
Fax: +1.415.486.2901

**European Office**
IdenTrust Inc.
288 Bishopsgate
London, EC2M 4QP
United Kingdom
Telephone: +44 (0)203.008.8330
Fax: +44 (0)203.008.8331