

# An Enterprise Perspective on Identity Theft

Who gets hurt. How we all contribute.

How your enterprise can be part of the solution.

This white paper explores the scope and roots of identity theft, how enterprises are victimized, and how they sometimes contribute, inadvertently, to the victimization of consumers. The discussion then turns to issues of accountability and “desired outcomes” and describes best security practices for thwarting identity-related crimes, with a focus on RSA Security’s identity management and encryption solutions.



# An Enterprise Perspective on Identity Theft

## Table of Contents

<b>I. Awareness:</b>	
<b>Identity Theft is Everybody's Problem</b>	<b>1</b>
A "Best Practice" for Criminals and Terrorists	1
Who Gets Hurt? Everyone But the Criminals	2
<b>II. Understanding and Accountability: How Did We Get Here? And What Needs to Happen Next?</b>	<b>2</b>
How Do We Stem the Rising Tide?	3
<b>III. Best Practices: RSA Security Helps Enterprises Fight Back</b>	<b>5</b>
Identity and Access Management Solutions	5
Strong Authentication: Verifying identity	6
Access Management: Controlling Who Has Access to What	6
Digital signatures: Authenticating Online Transactions and Communications	7
Encryption: Protecting Identity Data at Rest and in Motion	7
A Vision for the Future	9
<b>IV. Why Act?</b>	<b>9</b>
<b>About RSA Security</b>	<b>9</b>

## I. Awareness: Identity Theft is Everybody's Problem

Identity theft is as old as human history. From the Biblical story of Jacob and Esau, to the modern, true-life drama, Catch Me If You Can, there are countless tales of people impersonating others — almost always for personal gain, and often, with a darker criminal intent as well.

During the last several years, however, identity theft has taken on an even more insidious character. Enabled by network technology, it has grown from a specialized criminal craft into a huge and lucrative industry — one that is adept at maximizing revenues, minimizing risk and developing innovative ways to stay ahead of the competition (in this case, IT security measures and law enforcement bodies). Almost weekly, there are sensational accounts of large-scale thefts from businesses and government:

- 21,000 bank customers victimized by ATMs that “skim” users’ bank account numbers and PINs,
- 30,000 consumer credit reports stolen from a credit reporting agency, resulting in \$2.7 million in losses to credit issuers,
- 265,000 Social Security numbers (SSNs) stolen from a database of California employees, including the governor and state legislators,
- 8,000,000 credit card numbers stolen from a company that processes merchant transactions and
- A rise in high-end bank fraud worldwide, with single incidents netting as much as \$1 million.

Putting a personal face on these grim statistics, consumers recount how their lives, reputations and sense of security have been devastated by identity theft and the crimes that follow in its wake. Adding insult to injury, many must devote considerable time and energy to restoring their good name.

While estimates vary widely, there is no doubt that identity theft is widespread, fast growing and costly to society. In September 2003, the Federal Trade Commission (FTC) reported that identity theft had affected nearly 10 million Americans and cost almost \$53 billion in the previous year. Reported incidents increased 73% from 2001 to 2002 and accounted for 43% of the complaints fielded by the FTC. Worldwide, identity theft and related crimes are projected to cost an estimated \$221 billion in 2003, and experts believe the problem will get worse before it gets better. If the current 300% compound annual growth rate continues, annual losses worldwide could top \$2 trillion by 2005.<sup>1</sup>

---

<sup>1</sup>Source: Aberdeen Group, as reported in CIO Magazine, May 23, 2003.

### A “Best Practice” for Criminals and Terrorists

Identity theft is not simply one category of crime. It is the foundation for many crimes and it offers the perpetrator a rather remarkable set of benefits. Identity fraud:

- Allows criminals to conceal their true identities from the community and authorities, leaving them free to pursue illicit activities without arousing suspicion,
- Provides financial support, in the form of fraudulent loans and credit card purchases and
- Makes it more difficult to identify the perpetrator and prosecute a crime after the fact.

For all these reasons, identity theft has become a “best practice” among criminals and terrorists.

**Financial crimes.** Identity information is most often used to commit a string of financial crimes in the victim’s name. This may include financing foreign travel, purchasing luxury goods (which can be used or sold for cash), leasing a car or obtaining a mortgage and stealing the funds — obligations that will never be repaid. Many career criminals finance their lifestyle in this way, inhabiting one identity after another, or several at once.

**Felonies.** Identity theft also allows criminals to commit more serious offenses and deflect blame to the person whose identity has been stolen. The Washington Post reported on the case of Michael Berry, whose identity was appropriated by a convicted murderer. While living under Berry’s name, the imposter ran up thousands of dollars in credit card bills and murdered a neighbor. When the case was highlighted on the show “America’s Most Wanted,” Berry’s name was listed prominently as an alias and his Social Security number was displayed on national TV.

**Terrorism.** Terrorists use identity crimes to “hide in plain sight” and finance their global operations.<sup>2</sup> The September 11<sup>th</sup> hijackers used phony Social Security numbers and birth dates to establish residency in the U.S. A suspected al Qaeda associate, arrested at the U.S.-Canadian border with explosives in his car, told authorities he supported himself through credit card fraud and trafficking in identity documents. As one terrorism expert explained, “Identity theft — credit card theft, bank fraud — is hugely important to al Qaeda, as it is to many terror groups... Every time you arrest one of them he has 20 different identities and 20 different credit cards.”<sup>3</sup>

---

<sup>2</sup>All the details related to terrorism listed here were reported in the Washington Post, August 19, 2003.

<sup>3</sup>Attributed to Magnus Ranstorp, director of the Center for the Study of Terrorism and Political Violence at the University of St. Andrews in Scotland, as reported in Newsweek magazine.

**Online attacks.** Identity theft, particularly the fraudulent use of online identities, also facilitates online crimes: industrial espionage, computer hacking, cyber-terrorism, large-scale network attacks and, yes, the theft of identity information. One of the main culprits here is the widespread practice of using passwords as the sole means of establishing and authenticating an individual's online identity.

Notoriously easy to steal or guess, passwords enable an intruder to access any resources the legitimate user is entitled to see and to probe the entry points to more secure resources — all with little fear of being detected. For example, in Australia, a disgruntled consultant spent two months working his way through network defenses for a waste management control system, until he succeeded in releasing 800,000 liters of raw effluent — on his 46th attempt.

New, fast-spreading computer viruses amplify the risks posed by passwords. The Fizzer and Bugbear.B worms covertly install a keystroke logger on target systems and automatically send passwords and other personal information to a data collection point, thus facilitating future identity crimes. Additionally, both worms install a “back door” on the system, allowing an intruder to gain access at a future time. This transforms the victim's computer into a platform that can be commandeered to participate in distributed Denial of Service (DoS) attacks.

### Who Gets Hurt? Everyone But the Criminals

The many costs of identity theft are spread across all sectors of society, with the nature of the burden varying from sector to sector.

**Consumers bear the emotional costs.** Ultimately, most consumers are not held accountable for fraudulent transactions. Of the estimated \$53 billion annual price tag for this crime, consumers only account for \$5 billion — less than 10%. Yet they often bear a tremendous emotional cost.

First, the individual's credit reputation is ruined, making it difficult to buy a house, arrange an auto loan or change jobs. (Credit reports are often used to screen job candidates.) In extreme cases, an ordinary citizen may find his own name associated with serious crimes. As victims attempt to set the record straight, they must deal with a credit industry that appears irresponsible in its business practices and unresponsive to victims. Many victims must spend hundreds of hours and thousands of dollars on efforts to restore their good name. They are further frustrated by a criminal justice system that lacks the expertise and the resources to prosecute identity-related crimes. Many end up feeling re-victimized by this process, using words like “haunted,” “devastated,” and “violated” to describe their ordeal.

**Enterprises bear the financial cost.** Enterprises, especially financial services firms, bear the lion's share of the direct losses that result from identity-related fraud. The FTC estimates that last year U.S. businesses absorbed \$48 billion of the estimated \$53 billion annual price tag for identity theft. (As mentioned, consumers accounted for the remaining \$5 billion.) Because many companies are reluctant to disclose security breaches, those numbers surely understate the case.

In addition, companies that suffer highly publicized, identity-related security breaches are likely to experience a range of other negative effects including loss of brand equity, customer defections, lost business opportunities and costly litigation. Furthermore, they typically must bear the cost of implementing more robust security measures to avoid a repeat of the breach.

E-business growth is another casualty of identity theft. With awareness of identity crimes at an all-time high, consumers are unlikely to expand their use of online stores and services until they are persuaded that the security situation has improved significantly.

**Civil society is undermined.** Though impossible to quantify, the costs to society are enormous. By helping to conceal and sustain terrorists and criminals, identity crimes threaten our physical security. As the 9/11 terrorist attacks showed, this concealment can have devastating consequences, resulting in a staggering loss of life and seismic economic disruption. Furthermore, the direct and indirect financial costs of more prosaic identity crimes exert a drag on the economy, slowing growth and diverting resources that could be used more productively. In large ways and small, identity crimes undermine our collective sense of fairness and our trust in government's ability to protect us from predatory elements.

## II. Understanding and Accountability: How Did We Get Here? And What Needs to Happen Next?

Deeply systemic in nature, identity theft is an outgrowth of our information-driven society. Over the course of a lifetime, the typical citizen willingly surrenders personal information to dozens or even hundreds of different entities. All this data ends up being stored electronically, in countless locations, and often with little protection. Additionally, identity information travels freely through the traditional mail system — for example, in the form of credit card offers and bank statements — where it can be easily diverted.

As a result of this wide distribution, even those individuals who don't own a computer are vulnerable to theft. Identity information can be stolen by neighbors, roommates or troubled family members; by an unscrupulous colleague who

knows our habits; or by a merchant who copies down our credit card numbers. Low-tech thieves rummage through mailboxes and dumpsters and high-tech thieves pilfer corporate databases. Recently there has been a dramatic increase in scams that use official-looking but fraudulent e-mail, web sites and hard-copy documents to trick people into disclosing sensitive information.

Whether identity information is stolen by high-tech or low-tech methods, technology often facilitates and accelerates the crimes that ensue. For example, stolen personal information is often sold to third parties via shadowy web sites and credit card numbers can be used to make purchases online in a matter of minutes. At this point the real costs begin to mount for consumers and enterprises.

### How Do We Stem the Rising Tide?

Identity theft is a complex phenomenon that calls for vision and leadership across all sectors. A multi-level response is required, one that addresses the various dimensions of the issue: laws and public policy, business practices in key industries; IT security practices; procedures for helping victims restore their good name; the response by law enforcement and the criminal justice system; and changes in consumer behavior.

Thanks to heightened awareness around identity theft, there is much activity in all these areas. However, the remainder of this paper will focus on two critical and closely related aspects of the problem: protecting online identity data from being stolen or otherwise compromised and preventing the fraudulent use of online identities for the purpose of committing other crimes. Section 3 discusses how RSA Security solutions help address these two challenges.

**Desired Outcome: Enhance accountability among enterprises and government.** As simplistic as it may seem, one of the first steps in combating identity fraud involves all parties taking responsibility for doing their part. While recognizing that consumers have an important role to play, RSA Security President and CEO Art Coviello has advocated for enterprises and government to “step up to the plate” and show greater leadership and accountability than they have in the past.

Speaking and writing frequently on the topics Coviello has said, “It’s not an either/or situation. Individuals need to recognize how easy it is for someone to obtain their personal information and they need to take appropriate precautions. However, the majority of the burden needs to fall on the organizations that ask for and hold personal information. Companies need to acknowledge that it is a privilege to have access to the personal information of customers, employees and partners — and with that privilege comes an obligation to protect consumer information from being misused.”

---

*“Companies need to acknowledge that it is a privilege to have access to the personal information of customers, employees and partners — and with that privilege comes an obligation to protect consumer information from being misused.”*

---

**Desired Outcome: Enhance protections in key “enabling” industries.** While all organizations need to take accountability for battling identity fraud, certain industries tend to be at the nexus of identity-related crimes and, for this reason, require even greater vigilance. These industries include:

- Credit reporting agencies (CRAs), which hold extensive data on individual consumers and are thus an inviting target for identity thieves;
- Credit issuers, who, in some cases, do not carefully vet consumer identities and, as a result, repeatedly issue credit to fraudulent parties; and
- Wireless phone companies, banks, retail estate firms and state departments of motor vehicles (DMVs), who often facilitate the early stages of identity fraud. (To quickly establish a local identity, thieves will do business with all these sectors under the stolen identity — unchallenged by any of these parties — and then move on to larger crimes.)

By strengthening their practices for validating the identities of people they do business with and by implementing procedures to quickly recognize fraudulent behavior, these sectors could help choke off one major avenue for perpetrating identity-related crimes.

**Desired Outcome: Develop an understanding of how information is gathered and used.** For organizations that are committed to fighting identity theft, a key step is to examine how consumer and employee identity information is currently collected, stored and used across the enterprise. For example:

- What identity information is routinely gathered? Is it actually used for business purposes or just stored and forgotten? If sensitive information is being used, such as Social Security numbers, could the same business purpose be achieved using a less sensitive data point?
- How many different places is identity data stored and what kind of risk does that pose? What protections have been put in place? Is the data encrypted in transit and at rest?

- Who, among your employees and partners, has access to the information? How carefully are they screened and trained? What authentication methods do they use: Passwords? Or more secure methods? How are users' access privileges managed and tracked? Are your partners' security measures as rigorous as your own?

**Desired Outcome: Evaluate vulnerabilities to online identity fraud.** In addition to understanding where identity data is vulnerable, organizations need to assess their potential exposure to the fraudulent use of online identities. How many of your mission-critical resources — networks, applications and data sources — are only protected by passwords? How easy would it be for a hacker or other intruder to steal, guess or crack a legitimate user's online identity? What kinds of resources could they access simply by gaining entry to your intranet? How likely would it be that such an intruder would be detected and caught? How much damage might they do before drawing attention? How easy would it be for a legitimate user — such as an employee or partner — to commit illicit acts and escape detection?

Through this assessment process, an enterprise gains a baseline understanding of their current environment and vulnerabilities and can begin to redesign business and IT security practices to reduce their risk of identity theft and online identity fraud.

**Desired Outcome: Implement best security practices to thwart identity fraud.** Organizations that profess to take identity fraud seriously need to “walk the talk,” safeguarding customer information with the same high level of protection that is applied to sensitive proprietary information or high-value transactions. This means employing best security practices, such as the latest firewall and anti-virus measures. In addition, there are two critical areas where RSA Security technology offers industry-leading solutions.

- With identity and access management (I&AM) solutions, organizations can create trusted online identities, making it easier to reliably verify with whom they are doing business and allowing them to efficiently manage users' access to protected resources.
- Encryption solutions make data unintelligible to unauthorized users and, in the process, protect identity data from being compromised while at rest or in transit.

These RSA Security solutions are described in more detail in Section III.

**Desired Outcome: Achieve compliance.** Organizations need to understand how current laws and regulations constrain the use of sensitive information today and how pending legislation could impact business and IT security practices in the future. (For a representative cross-section of the most relevant laws, see “Relevant Laws and Regulations”)

**Desired Outcome: Develop cross-industry solutions for identity management.** As enterprises strive to enhance their internal protections against identity-related crimes, they are also working collaboratively to develop cross-industry approaches for creating, proving and managing online identities. The Liberty Alliance Project is one of the most far-reaching of these initiatives.

The Liberty Alliance is a global consortium of 150-plus businesses, government entities and technology



vendors. (RSA Security was one of 16 founding members.) The alliance was formed to develop a global standard for network identity management, based on the concept of federation: the ability of enterprises to securely share widely distributed identity information in a way that safeguards sensitive information and respects the privacy wishes of the consumer.

Ultimately, the goal is for each user to establish a highly secure online identity that would be recognized and accepted by a wide range of leading enterprises. Users would benefit from single sign-on (SSO) — the ability to navigate freely among protected e-business sites without having to register every time they encounter a new site or log in every time they return to a site. Businesses would benefit from the growth of e-business revenues, reduced partnering and process costs and faster deployment of innovative new services.

**Desired Outcome: Educate consumers and strengthen enforcement and penalties.** Even as enterprises seek long-term remedies for identity fraud, consumer awareness remains one of the most effective tools for battling identity-related crimes in the short run. As the Federal Trade Commission has documented, prompt discovery of identity theft dramatically reduces the total monetary value of fraud that is committed in a consumer's name. Early disclosure also reduces the amount of time and money the consumer must devote to repairing his/her credit reputation.<sup>4</sup>

With these facts in mind, more than a dozen leading companies and trade associations banded together in September 2003 to form the Coalition on Online Identity Fraud. Founding members include well-known technology companies and online merchants (Amazon.com, eBay, Visa, Microsoft), leading security technology firms (including RSA Security and McAfee Security) and two major industry groups, the Business Software Alliance and the Information Technology Association of America (ITAA). The coalition plans to address four primary areas:

---

<sup>4</sup>For example, when the misuse of the victim's identity was discovered within five months, the value obtained by the thief was less than \$5,000 in 82% of the cases. If six months or more elapsed, the loss was under \$5,000 in only 44% of the cases.

### Relevant Laws and Regulations

In response to the rising tide of identity theft and more general concerns about personal privacy and security, governments around the world have enacted identity-related legislation that has clear implications for IT security. A cross-section of relevant statutes and directives — including two California laws that offer a preview of things to come on the national level — follows.

**Disclosure of identity theft and related fraud.** The California Data Security Act requires state agencies and commercial enterprises that do business in California to disclose to California residents any time that their unencrypted personal information has been compromised or is suspected of having been compromised.

**Protection of Social Security numbers.** The California Law on SSN Confidentiality prohibits companies from using SSNs as passwords for logging into web sites. The law also prohibits the transmission of SSNs over the Internet unless the connection is secure or the number is encrypted.

**Protection of health and personal information.** The federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 defines standards for safeguarding the privacy and security of medical records and other individually identifiable health information.

**Protection of personal financial information.** The Gramm-Leach-Bliley Act defines requirements for financial institutions to protect the privacy and security of customers' personal financial information. The Financial Institution Privacy Protection Act would stiffen Gramm-Leach-Bliley to make company officers and directors liable for up to \$10,000 for each privacy violation.

**Transmission of personal data across borders.** European Commission Directive No. 95/46 sets standards for ensuring adequate protection of personal data that is transferred from EU countries — which have rigorous privacy requirements — to non-EU countries.

**Use of electronic signatures to authenticate online transactions.** Worldwide, there are numerous laws that govern the use of electronic signatures as a means of authenticating documents and transactions. These include the EU Directive on Electronic Signatures, the Japanese Law Concerning Electronic Signatures and Certification services, the aforementioned HIPAA and others.

As the costs of identity theft continue to rise and its mechanisms become more clearly understood, further legislation is sure to follow, creating new compliance requirements. Enterprises that anticipate these developments and implement best security practices today, will find themselves well positioned when new compliance requirements take effect.

- Educating consumers so they can protect themselves more effectively,
- Promoting technology and self-help approaches for dealing with identity theft,
- Sharing information about emerging online fraud techniques and
- Encouraging more effective enforcement and penalties for identity-related crimes.

### III. Best Practices: RSA Security Helps Enterprises Fight Back

For enterprises, there is some good news about identity theft: At least, we're not starting from scratch. Many of the investments that have been made in e-security during the last few years can be leveraged to address identity-related crimes and abuses in the online world. Organizations that adopt a more consumer-aware view of identity theft will suddenly see new opportunities to protect their customers and employees by making incremental adjustments to their current security plans.

RSA Security is well positioned to help organizations make this shift. Our industry-leading e-security solutions address two of the most fundamental and challenging aspects of identity theft:

- Creating and managing trusted online identities and
- Protecting sensitive identity information from compromise by using encryption technology.

#### Identity and Access Management Solutions

The concept of "trusted identity" is at the very heart of e-business, yet trust in the online environment is dismally low. RSA Security is helping enterprises rebuild that trust with its identity and access management (I&AM) solutions. These solutions enable organizations to create, manage, authenticate and authorize trusted identities, which can then be applied to any and all applications, data sources and transactions within the extended enterprise.

### Strong Authentication: Verifying identity

Increasingly, organizations are recognizing that authentication — the ability to reliably verify user identities — must be the foundation for online services and business practices. Unless you know who is on the other end of a network connection, all other protections are illusory. Organizations also recognize that weak passwords are simply inadequate to the task. Strong authentication is required to provide a high degree of certainty that online users are, in fact, who they claim to be.

Building on years of experience in this field, RSA Security offers strong authentication solutions that help ensure the authenticity of people, devices and transactions. Diverse options can be flexibly combined to meet differing requirements for security, scalability, user convenience, mobility and total cost of ownership.

- Easy-to-use RSA SecurID® hardware and software tokens create a barrier to unauthorized access through two-factor authentication — that is, requiring physical possession of a device that generates frequently changing access codes, combined with an individual's unique PIN code.
- One-time-use RSA® Mobile access codes, which are delivered to mobile devices such as PDAs and cell phones,

leverage existing mobile infrastructure, enabling enterprises to more securely extend popular web applications while reducing the risk of fraud.

- RSA SecurID smart cards combine the functionality of physical and network access into a one device, securing access to all corporate resources in a convenient and cost-effective manner.
- The RSA Keon® family of digital certificate management solutions offer scalable and portable authentication for legally binding electronic communications and transactions.
- RSA ClearTrust® web access management software provides advanced capabilities for creating, managing and authenticating passwords.

### Access Management: Controlling Who Has Access to What

Once users are authenticated, RSA ClearTrust software provides powerful, flexible capabilities for managing users' access privileges. This helps ensure that users can tap all the resources that are relevant to their relationship (customer, employee, partner, etc.) and role (purchasing manager, HR specialist, software engineer, etc.) or specific attribute (account status, clearance, etc.). At the same time, it bars users from accessing resources they are not entitled to use.

## REFCO

### Best Practices: Financial Services

REFCO Group Ltd., LLC is a world leader in risk management and investment services with operations in 14 countries, \$20 billion in assets and 180,000 customer accounts. To assist investors in making informed decisions, the company provides online access to account statements, research reports and other financial information.

With several lines of business developing their own web initiatives, REFCO was having a difficult time managing the security measures necessary to authenticate users and control their access to information. Users had to establish different online identities for different applications, resulting in an inconvenient user experience, inconsistent security practices across applications and high costs for managing authentication and access.

To address this challenge, REFCO deployed the RSA ClearTrust web access management software, which provides powerful capabilities for centrally managing user identities, authentication policies and user privileges across multiple applications and domains. REFCO was able to

implement single sign-on (SSO) for two of the more frequently visited areas of the REFCO web site: account statements and research. Because the RSA ClearTrust software offers seamless interoperability with REFCO's existing resources, implementation was quick and easy.

REFCO saw immediate benefits. Before RSA ClearTrust software was implemented, REFCO customers who wished to apply for a loan or financial program had to fill out a new application for each program. Now customers only need to fill out one application and simply check off the services they wish to apply for, a significant convenience.

As Frank Stearns, REFCO's web development manager explained, "RSA ClearTrust software enabled us to provide an architecture that would allow different REFCO businesses to develop their own web domains yet allow a centralized IT department to handle security and cross-domain authentication. As a result, we are able to focus on our mission of empowering investors with the information they need to facilitate informed decision-making."

In addition to enhancing security in these ways, RSA ClearTrust software increases user convenience, enabling secure, single sign-on (SSO) across multiple applications and domains.

Centralized access management is particularly valuable in establishing accountability for individuals who are entitled to be inside the firewall — including employees, partners and suppliers. By establishing an audit trail for all access attempts, enterprises are able to hold both users and administrators accountable for their actions. Delegated administration capabilities further enhance security by allowing internal business units and third parties to administer their own users. Moving administration closer to the user results in more fine-grained control of user privileges and a larger community of administrators alert to possible wrongdoing.

### Digital signatures: Authenticating Online Transactions and Communications

Digital signatures, which utilize digital certificate technology, are emerging as an effective method for authenticating online transactions and interactions that have traditionally required written signatures. RSA e-Sign technology, which is a standard component of the RSA Keon certificate management environment, enables organizations to capture binding signatures within end-to-end electronic processes, thus eliminating the delays, inefficiencies and lost opportunities that result when hand-written signatures must be obtained.

With RSA e-Sign technology, organizations can implement digital signature capabilities for online forms and e-mail. For example, secure e-mail solutions enable users to encrypt and digitally sign e-mail messages and attachments so that only the intended recipient can access the contents and any attempts to tamper with the message in transit will be evident. This transforms e-mail, which is notoriously insecure, into a trusted medium for communicating sensitive information (including identity information) and for conducting legally binding transactions online. Wide adoption of secure e-mail could also help undermine certain types of online fraud such as “phishing” scams that entail e-mail messages purportedly sent by legitimate companies.

### Encryption: Protecting Identity Data at Rest and in Motion

It is common for enterprises to store thousands or even millions of sensitive identity records in a single database — making it an inviting target for thieves. Implementing strong authentication and/or web access management significantly strengthens protection for the consumer information held in such databases. However, encrypting the contents of a database will further deter misdeeds by making data unintelligible to unauthorized users and extremely difficult to decipher when attacked. For example, even if a thief were to access a customer database, he would not be able to

## Blue Cross and Blue Shield

### Best Practices: Health Care

Blue Cross and Blue Shield of Kansas City is the largest provider of health plans in a 32-county area encompassing greater Kansas City and Northwest Missouri. The organization’s intranet/extranet serves several distinct populations: nearly 1,100 employees, more than 800,000 members, plus employers, healthcare providers, brokers and suppliers — all requiring access to different types of information.

To serve this diverse population effectively, Blue Cross and Blue Shield of Kansas City wanted to require different methods of authentication and provide different levels of access, based on the user’s role. Additionally, they needed to support compliance with the Health Insurance Portability and Accountability Act (HIPAA), which defines requirements for protecting the privacy and security of patient health information.

For employees who need to work remotely and access highly sensitive patient data, Blue Cross and Blue Shield of Kansas City issues RSA SecurID tokens, which provide strong authentication when logging in to the organization’s network through a virtual private network (VPN). “Passwords weren’t enough for us to feel we were doing everything possible to lock down our confidential information,” said Kurtis Keling, senior security analyst at Blue Cross and Blue Shield.

With the RSA SecurID solution, a user validates his or her identity by supplying two “factors” or identifiers: something only the user knows (a PIN) combined with something only the user has, in this case a 6-digit code that is displayed on the RSA SecurID token and changes every 60 seconds. This combination helps assure that only authorized users are granted access to confidential healthcare information.

Additionally, using RSA ClearTrust software, administrators were able to centralize and automate user access privileges for those accessing the intranet/extranet. “RSA ClearTrust software was the most logical choice for user privilege management and web single sign-on (SSO) because of its platform flexibility and fast implementation,” said Keling. “Now, our doctors, staff and patients can easily get the information they need while we control the information they can access.”

interpret the encrypted data — thus never ascertaining the real value of the information. RSA Security encryption solutions are also instrumental in protecting data that is in transit across networks. Again, if a transaction involving personal information, credit card numbers and passwords were intercepted, the fraudster would not be able to translate the encrypted data into meaningful information.

RSA BSAFE® technology has helped leading organizations implement encryption strategies that balance the need for robust protection and responsive performance. There are approximately one billion RSA BSAFE-enabled applications in use worldwide.

### Fighting Back: How RSA Security Solutions Help Combat Identity Theft

Online risks	Intruder's Objective	Technology Solution	RSA Solution
Fraudulent use of another's online identity (enterprise)	<ul style="list-style-type: none"> <li>Steal identity data, proprietary information, business plans</li> <li>Commit online attacks or scout future attacks</li> <li>Disrupt critical infrastructure</li> </ul>	Strong authentication Access management	RSA SecurID® RSA® Mobile RSA Keon® RSA ClearTrust®
Fraudulent use of another's online identity (consumer)	<ul style="list-style-type: none"> <li>Gain access to personal data</li> <li>Make fraudulent online purchases</li> <li>Commit online banking fraud</li> </ul>	Strong authentication	RSA SecurID RSA Mobile
Exposure of data at rest	<ul style="list-style-type: none"> <li>Steal consumer or employee data</li> </ul>	Strong authentication Access management Encryption	RSA SecurID RSA Mobile RSA Keon RSA ClearTrust RSA BSAFE®
Interception of data in transit	<ul style="list-style-type: none"> <li>Steal credit card numbers, SSNs, passwords</li> </ul>	Encryption Digital signing	RSA BSAFE RSA® e-Sign
"Phishing" scams and other ploys that ask users to input personal data	<ul style="list-style-type: none"> <li>Steal SSNs, credit card numbers, etc.</li> </ul>	Digital signing	RSA e-Sign
Keystroke loggers covertly installed by a worm	<ul style="list-style-type: none"> <li>Steal passwords and personal information</li> <li>Install "back door" for future access and DoS attacks</li> </ul>	Strong authentication	RSA SecurID RSA Mobile RSA Keon

### A Vision for the Future

These RSA Security solutions have evolved from the company's long heritage in authentication, access management, administration and encryption. Building on this rock-solid foundation, RSA Security offers a vision and migration path to the identity management system of the future. Code named NEXUS, this system will integrate today's proven solutions onto a single platform that delivers a common set of services across all RSA Security enterprise products. The initial set of services will include:

- User management services,
- Identity authority services,
- Access authority services,
- System services and
- Network and application integration services.

Components of NEXUS are already available in current RSA Mobile and RSA ClearTrust solutions and will continue to be rolled out in subsequent product releases. Integrating seamlessly with existing e-business capabilities and emerging web services, RSA Security solutions will continue to enhance security, improve the user experience and reduce costs associated with identity management.

### IV. Why Act?

Confronted as they are with many competing agendas and priorities, enterprises may well ask: Why respond now to the crisis of identity fraud? Why not wait and see how things evolve and then leverage the solutions that others develop? RSA Security believes there are three compelling reasons to address this challenge now.

- **Accountability.** First, it is the ethical thing to do. Individuals have entrusted their personal information to large organizations and are extremely vulnerable as a result. Enterprises, which benefit greatly from such information, need to take responsibility for better protecting that information. They also need to recognize that doing little or nothing is, in fact, an irresponsible practice that puts consumers in harm's way.
- **Risk.** By failing to safeguard against identity-related crimes, organizations increase the likelihood of security breaches and all the resulting costs: bad publicity, customer defections, lost business opportunities, remedial costs and legal liability. With the accelerating pace of online incidents, this risk appears to increase almost daily.
- **Opportunity.** The security measures that are most effective in thwarting identity-related crimes have a much wider strategic benefit. By creating an e-business environment that is viewed by consumers and businesses as being truly trustworthy, such practices accelerate the growth of e-business. In turn, this creates new opportunities to increase revenues, reduce costs and deliver innovative services that confer a competitive advantage.

### About RSA Security

With more than 12,000 customers around the globe, RSA Security provides interoperable solutions for establishing online identities, access rights and privileges for people, applications and devices. Built to work seamlessly and transparently in complex environments, the company's comprehensive portfolio of identity and access management solutions — including authentication, web access management and developer solutions — is designed to allow customers to confidently exploit new technologies for competitive advantage. RSA Security's strong reputation is built on its history of ingenuity and leadership, proven technologies and long-standing relationships with more than 1,000 technology partners. For more information, please visit [www.rsasecurity.com](http://www.rsasecurity.com).

# An Enterprise Perspective on Identity Theft



RSA Security Inc.  
[www.rsasecurity.com](http://www.rsasecurity.com)

RSA Security Ireland Limited  
[www.rsasecurity.ie](http://www.rsasecurity.ie)

BSAFE, ClearTrust, Keon, RSA, RSA Security, the RSA logo and SecurID are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other products or services mentioned are trademarks of their respective owners.  
©2003 RSA Security Inc. All rights reserved.

IDT WP 1003