Identity Theft: Who Are You Anyway?

Ralph Spencer Poore, CISSP, CISA, CFE

When farmer Jones walked into the general store in town, the storeowner — or one of his employees — would greet him personally. The storeowner knew whether farmer Jones' credit was good, what his buying habits were, and how he would settle his account. If someone else came in pretending to be farmer Jones, he had to look and act like farmer Jones, and if he didn't pull it off, he risked physical detention. Of course, there may be places today that are like the television show Cheers where everyone knows us. In cyberspace, however, our computer has a better chance to be known than we do.

The degree to which I must convey who I am to others directly correlates with the requirements of the transaction I attempt. Many transactions do not require me to identify myself. When I walk into a convenience store to buy a gallon of milk and I pay cash, the clerk neither requests nor needs my identification. When I attempt a transaction for which personally identifiable information is required (e.g., one requiring that I be at least 21 years of age), then either the clerk must ask for identification sufficient for the transaction or the clerk must acquire sufficient validation by personal recognition. The latter choice (e.g., recognizing that a man with a graying beard is probably older than 21) is, at least currently, not an available choice to online merchants. In cyberspace, the apparent identity (usually obtained from the hardware or software used) becomes your identity for purposes of an online transaction.

From knowing the identity of the computer presented, you may correctly identify the person using the computer — or not. Many technologies purporting to identify and to authenticate a person (“end user”) rely on the assumed relationship the user has with the computer that the user appears to be using. Cellular telephones and similar handheld computers (e.g., PDA) usually authenticate as if they were the end users. Successfully cloning such computers equates to stealing the identities of the legitimate owners — if only for limited purposes. Files used to authenticate a user can usually be copied to other computers. In Windows systems, for example, these
Solving the identity theft problem requires both knowledge of how identities are authenticated and what techniques are used for identification. When weak means of authentication are used, a perpetrator has a better chance of a successful masquerade. When the technique used for identification actually identifies an entity that may not represent the person the technique alleges to identify, then an effective authentication of that entity may still prove incorrect in identifying the actual user. For example, a public key infrastructure requires both trusted roots for certificate chains and trusted means for registering users. Services like Verisign and Entrust go to great lengths to protect the former, but may permit imposters to register. A recent and highly visible example of this was when two Verisign certificates were issued as being from Microsoft when Microsoft did not authorize Verisign to issue the certificates. The perpetrators successfully fooled Verisign into believing that they were Microsoft.

Relying on e-mail addresses, for example, as a means of identification, places the initial burden of authentication on the e-mail address issuer and a continuing burden on the system of controls that protect access to the authority to send an e-mail message using that address. Anyone can obtain an e-mail address. With some persistence, you can obtain an e-mail address that clearly represents someone else’s name. Few public e-mail systems require strong authentication of your identity before they will issue you an e-mail address. In fact, free e-mail services exist for which you need not present even a means of payment (e.g., credit card number or debit card number) through which a third party (in this case a financial institution) might vouch for you.

Private e-mail systems may fair no better. In a large accounting firm with which I am familiar, one or more persons unknown succeeded in obtaining or creating e-mail user identities that they used for at least 6 months (more likely over a year) before they were detected and shutdown. Many large organizations find when they perform an operational audit of user identifiers that active identifiers remain for people who have died, retired, resigned, or been fired. User identifiers may also exist through errors in the issuance process. For example, my company may issue rsmoore for me by mistake, and then, when a second request is submitted for rspoore (since I didn’t get my identifier), it is issued. With no one to complain about rsmoore, it may remain active. I believe each experienced information security professional and each experienced information systems auditor...
will know of examples of this problem. We rely at our peril on the issuer to ensure that a valid relationship exists between the user identifier (or e-mail address) and the true identity of the person using the identifier.

When the issuer takes seriously the need to authenticate the identity of the person to whom the issuer is issuing an identifier, we begin with an excellent foundation. Regrettably, the networks on which we rely, e.g., the Internet, may build poorly on that foundation. The address resolution process permits the rerouting of an e-mail message without the knowledge or consent of the person rightfully represented by the e-mail address. By hijacking a user’s messages, a perpetrator can impersonate either the originator or the recipient. Digital signatures and encrypted messages can diminish this risk but, as discussed previously, these techniques have weaknesses of their own.

Although we generally rely on e-mail addresses that we recognize as if they were valid surrogates for a person we know, we should remain skeptical — especially when acting on the message would transfer assets, potentially defame, or place people or property at risk. Unfortunately, almost any level of business reliance portends harm if misplaced. The huge success of e-mail, where control failures appear low, may desensitize us to the risk and cause us to lower our guard. The hacker certainly hopes this will be the case.

I KNOW WHO I AM AND I'M NOT THAT PERSON!

Mistakes happen. An incorrect billing statement, for example, could be a simple error, or someone might have pretended to be you. Forged credit cards remain a bane to credit card issuers everywhere. Credit card issuers spend millions of dollars on holograms, card validation codes, and alert services. The integrated circuit cards (IC, the so-called “smart” cards) are the latest response in an attempt to stem the billions of dollars in fraud and abuse of credit and debit cards worldwide. With the exception of IC cards and some aspects of alert services, the attempts at preventing card forgery — and the associated identity theft — only work when the card is presented to a properly trained and vigilant human for processing.

One of the most powerful tools in preventing crime is the assurance that the perpetrator will be apprehended. Although some people are sufficiently desperate that they attempt crimes that put them on camera, in front of witnesses, or create other, clear physical evidence that will be used against them, most of us fear getting caught enough (or have sufficiently strong ethical or moral sense) that we don’t commit such crimes. Cyberspace, however, tempts perpetrators by eliminating physical evidence at the scene of the crime and providing the perpetrator with a sense of anonymity. The science of computer forensics has advanced mightily as some perpetrators have discovered. Notwithstanding, the perception remains that getting caught for a cybercrime is unlikely. Weak identity controls and the perception that arrest is unlikely create a ripe environment for identity theft.

HOW DID I loose WHO I AM?

Identity theft can occur through the theft of card numbers, expiration dates, and your name. In most
instances, this is sufficient to permit telephone, Internet, or fax-based purchases. Some merchants now require some or all of the billing address for the card as a further check of the identity. In the case of persons who communicate this information to a merchant using a means that is not secure, the customer may compromise this data. Wireless telephones and HTTP instead of HTTPS are two examples that come to mind. To the extent that the merchant provides ineffective protection for the data after receiving it, the merchant may compromise this data. The CDUniverse loss of credit card records through an exploited security weakness is but one of too many examples. In several cases, e.g., U.S. Bancorp, a third party may have bought your data. If the acquiring third party’s controls prove ineffective, it may compromise this data. As weak as this system is, I am astonished that identity theft remains rare — and concerned that little exists to prevent it from becoming common. Ordinary use of personally identifiable information (PII) — without extraordinary care — places it in the hands of persons unknown who remain outside of the data subject’s control. With each such transaction you lose control over who you are. Generally, all that protects you is the lack of motive on behalf of those persons who gain access to your PII. In large organizations — even those with an excellent reputation for protecting customer data — there always seems to be at least one person with a motive. (For example, Bank of America’s alleged problem recently with an insider at a subsidiary who may have misused access to customer data by selling it to others.)

We potentially lose control of who we are with every transaction we make that includes a transfer of PII to someone else. In the United States, privacy (i.e., control over one’s own PII) is not treated as a human right; rather it is treated as a property right. Although much is said about privacy as a Constitutional right, the Constitution (including amendments) is silent on this matter. The U.S. Supreme Court has pieced together some elements of a right to privacy largely related to search and seizure and to abortion. Notwithstanding, both the governmental sector and the commercial sector buy and sell PII — and generally do so without the consent of the data subject. New laws, e.g., the Gramm-Leach-Bliley Act (GLB) and the Health Insurance Portability and Accountability Act (HIPAA), have the potential for mandating notice (at least in some cases), but they may produce more exceptions than protections (especially the privacy rules for HIPAA, finalized April 12, 2001). You may already have received “opt out” notices under GLB from your financial institutions. However, opting out may prove of limited value in protecting your “nonpublic personal information,” which is all that GLB requires a financial institution to protect. The exceptions permitted under GLB and the potential for control failures with each transfer of PII provide small comfort. In addition, an “opt out” is not retroactive. Data already sold or transferred to another organization remains gone.

WHERE DID MY identity GO?

With few exceptions, organizations are not required to keep records of their allowed transfers of PII. Even when they are required to do so, the granularity of that audit trail may prove less than useful. For example, just knowing that someone within a large company such as GE obtained your credit history is probably insufficient for tracing where it went. Without accurate audit trails, finding and correcting errors in PII can become a nightmare. Because organizations give precedence to computer databases over the testimony of real people, an error may result in
denied credit, denied employment, denied medical coverage, false arrest, improper medical treatment, defamation, unauthorized transfer of assets, and just plain bad things. Once your identifiable information leaves the firm to which you entrusted it, you've lost control. Just like closing the barn door after the horse has left, opting out proves an ineffective countermeasure once an organization has given, sold, or bartered your PII away.

**WILL I RECOGNIZE MY IDENTITY IF I FIND IT?**

While human error may associate errors with your identity and inadvertently cause you harm, people may exploit the poor recordkeeping and commercial market for PII to intentionally cause harm. By introducing false information into records associated with an individual, a perpetrator can create a false profile of that individual. The individual may only become aware of the false information after the information has spread to multiple databases. At that point, correcting the information may require Herculean efforts. Generally, the victim cannot recoup the costs associated with such corrective actions. The organizations duped into accepting the false information are also victims whose costs may go well beyond that of correcting the erroneous data. Any organization acting on such false information may create significant liabilities for itself, improperly allocate resources, or place assets at risk. As important as our identities are to each of us, their representations are essential to modern commerce. In fact, they have become so essential that our true identities are less important to commerce than are the representations made as our identities. If your earnings are reported under my Social Security number, then I will accrue the benefits — and probably the tax liabilities. If your name and date of birth are used to obtain credit, the fact that you knew nothing about it may not prevent an adverse credit report. And does your employer know you were arrested for prostitution and have HIV?

In cyberspace, who we are is unimportant. All that matters is who we appear to be. If the user ID and password are correct, that is who we are. If the digital signature verifies, that is who we are. If the name, account number, expiration date, and billing address we give matches what the company has on file, then we are that customer — even if we are not.

Biometrics may offer some help against identity theft. It certainly raises the stakes. How do I change my fingerprint, voiceprint, retina pattern, or even DNA if someone else gains the ability to use them? How do we protect against their misuse? All biometrics have the potential for being copied. A single cell or strand of your hair may prove sufficient to clone additional material with your DNA. The effectiveness of biometric identification depends on the effectiveness of the registration process and the security and controls over the authentication process. Associate a biometric with the wrong person and the person with that biometric becomes the person with whom its associated — at least until that person can prove through his actual biometric that he is not the person whose biometric points to him. In databases, this distinction will not exist. Computers relying on a biometric database will associate you with the entry you match. Thus, your biometric may point to an entry that is not who you claim to be or someone else's biometric may point to who you claim to be. In either case, who you are isn't who you are, is it? Try explaining to the police that the near perfect fingerprint match wrongly identifies you, especially when your fingerprints
don't match what the computer says are the fingerprints for the person you claim to be. The stronger the scientific basis for authentication, the more calamitous the result when the association breaks down.

**ANY IDEAS FOR PROTECTING MY PII?**

Individuals can take some steps to protect their PII. They can “opt out” at each opportunity. They can write their legislators to lobby for stronger laws. They can limit what PII they release. Many organizations ask for information beyond the minimum data needed for the conduct of a given business transaction. If you decline to provide it, the transaction is not impaired. However, some employees may have trouble dealing with fields left blank. Some computerized systems have trouble with fields left blank. If patience fails, then a willingness to boycott these merchants may prevail. Surrendering to their incompetence just rewards them for insisting on PII that they don’t need.

Although not releasing PII is your best protection, most of us already have PII at risk. Vigilance becomes the next best protective measure. Periodically review your credit bureau records. Carefully examine monthly billings for unauthorized or unexpected charges.

As information security professionals, we have an obligation to help our respective organizations protect PII. We need to assist our organizations’ implementations of privacy policy and procedures. In many organizations, the need for proper privacy policy and procedures flows from regulations. More and more, however, organizations are realizing the potentially devastating effect that public disclosure of poor privacy practices can have. Even organizations without regulatory incentive may find merit in protecting the PII they need for their business transactions. The clear need for appropriate privacy policy only acts to remind us that security measures must enforce the policy. Empty privacy promises portend more public-relations harm than good. To protect PII requires controls in at least the domains under your control including

- Transmission between computers
- Storage (regardless of medium)
- Processing

Cryptographic security methods, e.g., SSL or IPSEC, may address protection while in transit, and an organization can store PII in encrypted form. A secure platform for processing usually remains problematic. However, new technologies will address this as well. As information security professionals and information system auditors, we need to invest some of our CPE requirements in keeping current on the technology and the ever-changing legal front. Protecting the privacy of PII is essential if we are to reduce the risk of identity theft. We need to design systems such that they do not rely on surrogate identities, i.e., identities of products that might be used by someone other than the expected user, because relying on such identification increases the potential for identity theft. Most of all, we need to educate our respective organizations and the public to the risks of identity theft and to the countermeasures available.

**Note**

1. In 1999 U.S. Bancorp was sued by a group of State Attorneys General and a separate class-action lawsuit related to alleged release of customer account information to a third-party merchant. These actions were both settled in 2000 for a total cost to U.S. Bancorp (based on U.S. Bancorp’s press release) of over $7.5 million.