Technology, Business, and Government Fight Identity Theft

The low-cost availability of computer technology has made the work of identity thieves extremely easy. It seems only fair that technology might also hold the keys to winning the battle against identity theft.

High-Tech Tactics to Combat Identity Theft

Biometrics

The term "biometrics" is derived from Latin, meaning "life measurement," and it shows great promise in the battle against identity theft. The Fair and Accurate Credit Transactions Act of 2003 (FACTA) even contains a provision requiring the Federal Trade Commission (FTC) to study whether biometrics and other technological advances can be used to fight identity theft. Various biometric technologies that are being tested and used now include fingerprinting, ear printing, retina scanning, iris scanning, voice recognition, facial recognition, handwriting analysis, handprint recognition, and hand-vein geometry.

A recent version of the Android smartphone operating system uses a biometric facial recognition system to unlock the smartphone. The Apple iPhone's popular Siri system is just the first step in what is sure to be a voice recognition system in the future.

The Canadian company Bionym, Inc., makes a bracelet called Nymi that uses the wearer's heartbeat as a biometric identifier that is used to open car doors.

Disney World uses finger scanners when patrons enter the theme parks to prevent ticket holders from sharing tickets.

ATMs in Japan are already using scanners on to which the customer places his hand so that the scanner can read the unique vein pattern in the customer's hand in order to authorize any transaction.

Voice recognition systems have been developed by companies such as Nuance Communications and Agnitio. The systems analyze a hundred aspects of a person's voice. Concerns about an identity thief using a high-quality recording of a person's voice could be reduced by requiring the customer to say his or her name more than once. A real person would have some minor differences in his or her voice that could be recognized by the software, whereas a recording would always sound the same and should be recognized by the program.

At the heart of any effective biometric system is not just some sort of measurement of a unique physical characteristic of a person, but also the confirmation of that person's identity through comparison of those measurements with a readily accessible computer data bank of the measurements of the general population. The most famous existing database is the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which is capable of performing more than 100,000 comparisons per second—in 15 minutes it can complete a data bank review of more than 42 million records.

No system is perfect. In constructing any system there is always a delicate balance between the rates of false acceptances and false rejections. False acceptances occur when a person is wrongfully matched to someone else's biometric measurement maintained in the central data bank. False rejections occur when a person's biometric measurement fails to be matched with his biometric measurement maintained in the central data bank. Generally, manipulating the system to lessen false acceptances tends to increase the rate of false rejections, and adjusting the system to reduce false rejections causes an increase in the rate of false acceptances. In the real world, no system is perfect. When security concerns are highest, systems tilted toward minimizing false acceptances are usually used. When such a system is used, however, it is necessary to have a backup procedure for establishing the identity of someone who has been wrongfully rejected by the system.

A major security concern that should be addressed by any biometric identification system is to ensure that the database is protected from hackers gaining access to the central database system and switching or altering data.

Biometric Manipulation

An old computer axiom is "garbage in, garbage out," which means that when invalid data is entered into a computer system, the resulting output will also be invalid regardless of how good the system itself is. Whatever biometric system is used, a crucial moment for establishing the reliability of the system is the establishment of the database to which future measurements will be compared.

An identity thief who can compromise that initial step by, for instance, using a stolen Social Security number or a phony birth certificate in order to have his own biometric measurements assigned to someone else's identity, is at a tremendous advantage in utilizing identity theft for fraudulent purposes. Another opportunity for an identity thief to manipulate a biometric system is by having his measurements entered into the system as belonging to a number of different identities that he would utilize for criminal purposes.

Privacy Concerns

Privacy advocates are particularly concerned about whether the vast collection of identifying data necessary for an effective biometric system is worth the invasion of people's privacy and whether the system could be too easily misused to monitor the population by both government and businesses. It is a legitimate concern and one that must be dealt with in any discussion of the use of biometrics.

Voice Recognition

Voice recognition has the benefit of simplicity and being a noninvasive technology. Its drawbacks are that voices change over time and are subject to manipulation by a clever identity thief. Comedian-impressionist Rich Little would have had a field day if he had ever turned to the dark side of the force. In addition, there is the problem of a voice recognition system being manipulated by an identity thief with a tape recording of the voice of his victim.

The Future Is Now

Bank United of Texas has been using iris recognition instead of PIN numbers at its ATMs since 2000, and the reaction of consumers has been generally quite positive. Quite eye-opening. Unfortunately, for me iris recognition always brings back disgusting thoughts of Tom Cruise as Detective John Anderton undergoing a double eyeball transplant in the movie *Minority Report* in order to gain access to a building that uses iris scanning for identification purposes. The technology behind iris recognition is of fairly recent origin. Iris scanning not only is highly accurate, but also is a system that is relatively simple to operate. A video camera scans a person's eye from around 20 inches away and takes a picture of the iris, which is considered to be unique. Problems can occur, however, if the person's iris is dilated due to drug use or if colored contact lenses are worn. An advantage of iris scanning is that a reading can be compared to a database of iris records significantly faster than fingerprints due to fewer items within the scan having to be matched.

Ophthalmologist Frank Burch first proposed the use of iris patterns for personal identification as far back as 1936, but it was not until 1987 that ophthalmologists Aran Safir and Leonard Flom patented the idea. Algorithms created

by Cambridge University Professor John Daugman led to his creation of software that provides for the analysis of the multifaceted image of the iris.

When it comes to beating the system, criminals who are Tom Cruise fans would not be able to cut out someone's eye and hold it up to the camera to manipulate the test. According to Professor Daugman, when the eye is removed from the body, the pupil dilates significantly and the cornea turns cloudy, making this attempt to fool the system worthless.

Presently, iris scans are already starting to make inroads in criminal identification. The Barnstable County Massachusetts jail was one of the early users of this technology.

Retinal Scans

Of the new biometric identity techniques, retinal scans are probably the most accurate but far from the simplest for establishing an all-important initial database. Retinal scans measure the unique pattern of blood vessels in the eye. Retinal patterns generally remain constant during a person's entire life; however, diseases of the eye such as glaucoma or cataracts can change a person's retinal pattern. Unfortunately, at present the process for performing a retinal scan is time-consuming and cumbersome, requiring the subject to keep his or her head still, focusing an eye on a specific location while an infrared beam is applied through the pupil of the eye. The reflected light is then measured and recorded by a camera.

Fingerprints

One of the oldest and still most dependable forms of biometrics is fingerprinting. It is a tried-and-true identification system that is already in place, highly accurate, and cost-effective. But it is not perfect. The highly sophisticated FBI IAFIS still has a 2 percent to 3 percent false rejection rate. A number of states—California, Texas, Colorado, Oklahoma, Hawaii, and Georgia—already require drivers to provide a fingerprint when they get drivers' licenses or renew their licenses. The state of Washington has a voluntary system allowing fingerprints, retinal scans, and other biometric measures to be used when obtaining or replacing a driver's license.

Systems also already exist that could be used for fingerprint confirmation when applying for a driver's license, through which a person's finger would be placed on a scanner that would transmit the data to a main computer and compare the print to prints contained within its database. A match would bring up a photograph of the person that could be transmitted back to the Department of Motor Vehicles. If the picture matched the person applying for or renewing a license, the license would be issued. If it did not match, further inquiry would occur. The new driver's license issued using this procedure would carry a magnetic

strip such as is found on credit cards. In this case, the strip would contain a digital encryption of the fingerprint that could be used for future identity confirmation. One fly in this ointment is that if the information contained in the original database was tainted or compromised by an identity thief, anything flowing from that would be further corrupted.

Providing a new meaning to giving the finger to the check-out clerk, the Piggly Wiggly stores in some states already utilize a Pay by Touch system in which you place your finger on a scanner at the check-out counter to purchase groceries. The scanner measures 40 specific data points on your finger that are encrypted into a unique mathematical equation to identify you and also access your bank account.

Unfortunately, the very fact that fingerprinting has been with us so long also means that criminals have had many years in which to develop ways to beat that system. Applying glue to fingers before being fingerprinted can cover the skin ridges that make up a fingerprint, rendering it useless as an identifier. Common household cleaners can even be used to change ridges on the finger necessary for a readable fingerprint. Fingerprint readings can also be affected by dirt on the fingertips or the condition of the skin. Finally, both the taking of initial fingerprints and the matching process are activities that require a significant level of skill to be done correctly.

LOOK AT THAT FACE

Facial recognition is another noninvasive technology that is still in its infancy, but offers some promise. Some Internet banks are testing facial recognition systems that would use Web cameras to confirm the identity of bank customers seeking access to their accounts through their computers over the Internet. Unfortunately, in tests done by the Defense Department and the International Biometric Group, a research and consulting firm concluded that using present technology, correct matches are accomplished only about 54 percent of the time.[1] Facial recognition also has the drawback of being subject to too many sources of error, including effects of light, facial expression, and weight gain.

Business Fights Back

Business often is accused of not doing enough to reduce or stop identity theft. Some people believe that businesses consider it a cost of business that they just pass on to their customers. However, The Financial Services Roundtable, an organization of 100 of the largest financial service companies from banking to insurance to investments, has created a pilot project called the Identity Theft

Assistance Center to help combat identity theft. Victims of identity theft can make a single telephone call to their local bank that takes over from there and brings the Identity Theft Assistance Center into action. The Identity Theft Assistance Center contacts the identity theft victim and coordinates the drafting of an identity theft affidavit to be provided to law enforcement agencies, credit card companies, the credit-reporting bureaus, and other companies with which the victim does business. The Identity Theft Assistance Center also maintains a secure database of the names of identity theft victims. The database is available to financial institutions receiving credit or loan applications so that they can easily determine whether the name of the person requesting a loan or credit is the same as someone who has been reported as being the victim of identity theft.

Government Response

Identity theft was not even made a federal crime until 1998 with the passage of the Identity Theft Assumption Deterrence Act, which specifically criminalized identity theft. The law also required the Federal Trade Commission to keep records of identity theft complaints and provide victims with informational material. This law was followed by the Identity Theft Penalty Enhancement Act in 2004, which provided penalties for aggravated identity theft. Four years later, Congress passed the Identity Theft Enforcement and Restitution Act, which provided for restitution to identity theft victims for the time spent reclaiming their identities.

In 2006, President George W. Bush established the Identity Theft Task Force by an executive order in which he ordered 15 different federal departments and agencies to come up with a comprehensive strategy to combat identity theft. The Task Force submitted a plan to the president a year later, and in the years that followed, many of the recommendations made by the task force have been implemented. The Strategic Plan recommended by the Identity Theft Task Force focused on four distinct areas: data protection, avoiding data misuse, victim assistance, and deterrence.

One of the primary objectives of the Task Force was to reduce the unnecessary collection and use of Social Security numbers, which are so often the key to identity theft. Although much progress has been made in this regard, much still needs to be done within both the government and private industry.

In accordance with a requirement of FACTA, rules were enacted on identity theft "red flags" that are required to be followed by financial institutions and creditors to combat identity theft in both new and existing accounts. The new rules required the institutions to have reasonable policies and procedures for detecting and preventing identity theft.

Out of recognition that identity theft is a worldwide problem with many organized identity theft rings originating in foreign countries, American law enforcement is making an effort to work more closely now with foreign law enforcement to combat the problem. They are also working to identify countries that have become safe havens for identity thieves and are using diplomacy and other enforcement initiatives to achieve greater cooperation by the governments and law enforcement in these countries.

In 2008, through the joint efforts of American and Romanian law enforcement, a major identity theft ring based in Romania was busted.

In 2011, the federal government began the National Strategy for Trusted Identities in Cyberspace, which is an effort by the federal government to join with the private sector to create a new online user authentication system so that people could interact with the government online without including their Social Security number.

India has beaten the United States to the punch. In 2010, it started issuing biometric identifications to each of its 1.2 billion people. According to the Center for Global Development, there are already more than 160 biometric identification programs being used by countries around the world.

Although financial institutions are required to comply with security criteria established pursuant to the Gramm-Leach-Bliley Act, other businesses such as retailers are not subject to those security rules. Congressional failure to pass legislation to require greater cybersecurity actions by nonfinancial businesses resulted in the Obama Administration in 2014 issuing 41 pages of purely voluntary guidelines to provide a best-practices guide for banking, defense, utilities, and other vulnerable businesses. These guidelines provide best practices in regard to identifying, protecting, detecting, responding, and recovering.

Just Do the Best You Can

When I was a teacher at Old Colony Correctional Institution (a fancy name for one of the Massachusetts state prisons), one of my students was serving two consecutive life sentences. I asked him about that apparent contradiction. After all, how can you serve two life sentences? He first explained to me that he had the same thought at the time of his sentencing, and with apparent irritation in his voice had asked how the judge expected him to serve two life sentences, to which the judge responded, "Just do the best you can." My student later told me that the real reason for being sentenced to two life sentences was that if his appeal was successful on one of the crimes for which he was sentenced to life in prison, the state would still have the other sentence hanging over him.

I tell you that story because, unfortunately, with so much of your personal information found in the records of your employer, your accountant, your

lawyer, your doctor, your health insurer, your bank, and so on and so on, we are all vulnerable to a bad apple working in one of those offices. Identity theft can be as high-tech as a hacker breaking into a company's computer system from afar and stealing personal information or as low-tech as an identity thief going through your trash. The best you can do is to try to minimize your vulnerability and be vigilant and ready to respond if you discover a breach of security.

Endnote

1. Jonathon Phillips et al., "An Introduction to Evaluating Biometric Systems," *Computer* (2000), http://www.hh.se/download/18.70cf2e49129168da0158000129674/Intro_to_Evaluate_Biometrics.pdf.