RightNowWeb. Every query gets assigned a particular Web location, which is included in the automated email acknowledgement to the customer so one can find the message on the bank's Web site. More institutions should take advantage of similar technologies.

Several replies didn't really answer our query. Goldman Sachs took about eight hours to process our query, and then sent the following reply: "Thank you for visiting the Goldman Sachs Mutual Funds Website. You may visit the following link to request a prospectus and account application for any of our funds." All well and good, except no link was provided in the message. Chase also didn't answer our query, but gave a telephone number to call rather than any link on the Web. Morgan Stanley and PNC Bank both recommended we search their site, find the nearest branch and then call them directly. US Bancorp was the best of the bunch by saying, " Unfortunately we do not have a URL to send your request." At least they tried to answer our query.

If our results are any indication of the type of responses a typical customer experiences, most financial services firms have a long way to go before they can implement satisfactory customer service via the Web and email.

-DAVID STROM

Security

Cracking the Myths of Encryption

THOMAS JEFFERSON, A politically incorrect but brilliant founding father of the United States once wrote, "The price of Liberty is eternal vigilance." Eternal vigilance is also the price of Internet security, a fact that every business seeking to extend its sales into cyberspace should accept without question.

Until recently, most people believed that Internet security depended entirely on encryption. Better encryption was thought to guarantee better security. "That belief is changing," says Bruce Schneier, founder and head of Counterpane Internet Systems, Inc. in San Jose, CA.

Schneier should know. In 1993, he published Applied Cryptography, which showed programmers throughout the world protocols, algorithms and source code needed to write encryption algorithms, the locks used to safeguard access to Web sites.

Seven years later, Schneier says, " I learned that encryption alone is not the answer." Why not? Trained as a cryptographer and a mathematician, his experience with people who used his encryption codes led him to decide that secure codes alone will not protect a company. "People are worried about their locks, but they forget that while their doors are locked securely, their windows can be opened." Nevertheless, encryption code was a resource that was guarded carefully.

In the mid-90s, the U.S. Department of Commerce Bureau of Export Administration forbade U.S. software producers from exporting encryption software that was any larger than 28 bits.

Tom Monte, a Unix administrator with creditex in New York uses PERL for writing encryptions. PERL is a scripting language that he says does not have to be compiled like JAVA. "PERL used to have a T-shirt with a PGP key written in PERL so that if you wore it out of the country you could be arrested for illegal exporting," Monte recalls. Later, the encryption limit was raised to 56 bit. All in all, it was a curious policy since Schneier's book was published by Wiley which has offices on four out of seven of the world's continents.

Since then, the U.S. government has come a long way. In July, the White House announced that U.S. companies may now export any encryption product to

any end-user in the 15 European Union countries as well as eight other U.S. trading partners including Australia, Japan, and Switzerland.

There is considerable discussion about public key infrastructure. Law enforcement authorities want to hold a key to every encryption method which is typically composed of two parts; a "lock" one of the bank's servers, for example, and "key" form of a password. Singapore and Malaysia have recently authorized PKI. "We have insisted that our government use PKI," a Commerce Department spokesman said recently. However, it may be that PKI