Internet Banking & Fraud: Making Business Less Risky

By Mike Potter

As community bankers consider the scope and pace of their Internet delivery strategies, an appropriate risk management framework must also be considered so that strategy and technology may move forward effectively. This month's article was provided by the St. Paul, an alliance partner of the ACB Partners programs.

Most ACB members have either already begun or are contemplating offering Internet banking to their retail customers.

The booklet *Community Banks: A Competitive Force*, written by Grant Thornton LLP, provides an interesting statistic from Thornton's 1999 "Sixth Annual Survey of Community Bank Executives." The report states that 17 percent of community banks offer home banking via personal computer today and predicts that 82 percent are likely to offer it within the next three years.

One issue facing members when implementing a bank-at-home Internet strategy is whether the savings afforded by this electronic technology are sufficient to offset the costs—and risks—associated with the desired service capability offered to the bank's customers. One such risk is fraud by computer theft.

The risk of Internet computer fraud (ICF) increases as a bank expands its array of online services to its customers. In many arrangements, a bank will use a third-party service provider to grant Internet access to the bank's computer system. Both parties will use preventive and detective system controls as a defense to ICF.

Some members are at the informational stage of Internet banking. Here, existing and potential customers alike are provided marketing information on a stand-alone server. This capability doesn't require an electronic link between the server and the bank's own internal computer system. At this stage, ICF is generally either mischievous alteration or malicious destruction of content on the website.

The next level of interaction, communicative, usually allows customers to access their account balance and view account activity. This service level requires a link from the Internet server to the bank's own internal computer system, which creates a greater degree of risk for unauthorized entry of fraudulent data, be it a virus attack or manipulation/alteration of customer account data.

Finally, some banks provide transactional Internet access to their customers. This service level usually affords customers password-protected bill-paying and funds-transfer capabilities from their home PC. Most agree it poses the highest degree of risk to unauthorized activity by ICF.

Risky business

In the realm of Internet banking, inevitably, the following question arises. "What insurance coverage responds to the bank's liability for loss of customer funds caused by the unauthorized access and intentional entry of fraudulent data to a customer's account over the Internet?" Answer: a bank's financial institution bond or computer theft policy.

The principal coverage obtained by a community bank for the loss of customer funds arising from such acts usually will be within the financial institution bond under the computer theft insuring clause. Larger financial institutions may carry a separate computer theft policy. (Naturally, this coverage is subject to the General Agreements, Conditions and Limitations of the bond or policy that may apply based upon specific loss scenarios.)

In general terms, the coverage is designed to respond to loss of property resulting directly from computer/computer-related theft by a person (other than a bank employee) acting alone or in collusion with other non-bank employees. If that collusion proves to be with a bank employee or a bank employee commits the act, the bond's fidelity insuring clause will override the computer theft coverage.

The provisions of the computer theft coverage available to community banks within the St. Paul Financial Institution Bond spell out the protections provided to a bank if an unauthorized person gains access to a customer's account(s) and intentionally enters fraudulent data that results in a loss of customer funds.

First, the coverage relies on a definition of computer theft, which is defined as:

(a) an intentional, unauthorized and

fraudulent entry of data into a computer that creates an unauthorized data record; or

(b) an intentional, unauthorized and fraudulent change to data elements or program logic that is kept in machine readable format (including, but not limited to, unauthorized changes to data on disks, tapes or cards).

"Computer" is also defined as data processing equipment, communication lines (including telephone lines, coaxial cables, satellite, microwave, radio wave or fiber optic transmission), data elements and program logic, located:

(1) in an office of the insured;
(2) at service bureaus with whom the insured has contracted for data processing services (including other financial institutions); or
(3) at an automated clearing house (including a Federal Reserve Bank), "Switch" or other electronic communications system.

The data processing equipment, communication lines, data elements and program logic located at the bank or its contract electronic data processor (EDP) are addressed within (1) and (2) of the "computer" definition. Any third-party provider of a web server that provides the communications link between the bank and its customers is not considered an EDP under the terms of the bond.

Therefore, the threat of unauthorized computer access to customer accounts over the Internet (e.g., account balances) by a nonbank employee (commonly referred to as a "hacker" or "interloper") is intended to be covered by the computer theft insuring clause. The coverage addresses a customer's account data stored in a computer at the bank or at its authorized electronic data processor.

Prudent risk management procedures dictate that a community bank should periodically review with its independent agent its progress in using the Internet as a banking tool. Ensure that your security measures are reasonable for your situation and consider purchasing computer theft coverage as a risk-transfer vehicle to protect the bank against those risks associated with using the Internet.

Questions on Internet banking exposures and institutional coverage can be directed to Rich Thomas at The St. Paul, the institutional risk coverage resource for ACB members, at (651) 310-8285; rich.thomas@stpaul.com