

Identity Theft: Is it Covered?

Insurance policies are typically defined by the type of loss they cover. Identity theft—whether accomplished via hacking, phishing, dumpster diving or whatever the latest technology allows—is not in and of itself a loss to the bank. However, there are several types of losses that may ensue if a customer’s identity is stolen as a result of the bank’s failure to safeguard confidential customer information. To understand whether the bank is protected against identity theft, it is important to understand these exposures and ensure that the bank’s policies do not preclude coverage for the personal injury allegations associated with identity theft.

There are three potential losses that the bank may incur as a result of identity theft.

1 First party loss, whereby money leaves the bank and the bank incurs a loss of funds (either the bank’s money or a customer’s), is typically covered under the **Financial Institution Bond**.

Coverage for identity theft may be found under various insuring agreements, depending on how the loss was perpetrated. The most common remedies can be found under:

- › **Employee Dishonesty (Fidelity)**, if the fraud is perpetrated by an employee who has used access to customer records to embezzle funds;
- › **Forgery/Alteration**, if the perpetrator uses the information to counterfeit or otherwise collect on forged or altered negotiable instruments; or
- › **Electronic/Computer Systems coverage**, if the perpetrator accesses confidential customer information directly to move funds or submits transfer instructions by phone or electronically.

2 Third party loss occurs when the bank is sued due to its negligence in failing to safeguard confidential customer information, whereby such failure results in identity theft. Coverage for third party loss is typically found in the D&O policy; however,

- › **Broad Form Company Liability** coverage must be purchased to ensure that the bank is protected and not just the individuals;
- › Many D&O policies have an Internet or electronic banking exclusion, requiring the bank to maintain **Internet Banking Liability** coverage to protect against suits from unauthorized access to electronic data, including the Internet; and
- › Most policies maintain a personal injury exclusion that excludes allegations of invasion of privacy; **Privacy Liability** can provide coverage for claims of negligence in the management or oversight of confidential customer information.

3 Expenses will most likely be incurred by the bank to mitigate fraud and potential liability following an alleged breach of security.

These expenses may range from customer notification and card reissuance, to credit monitoring on customer accounts, and to public relations expense addressing negative publicity surrounding the breach. The sum of this expense can be daunting.

Privacy Liability Mitigation coverage can be purchased to reimburse these expenses, both under the D&O policy (for non-electronic breaches, such as dumpster diving and laptop theft) and Internet Banking Liability policy (for breaches involving the electronic arena).

Even the most security-conscious bank may be vulnerable to identity theft exposures, if confidential customer information is obtained from vendors, processors, or even naïve customers. Review your policies to ensure that your exposure is mitigated to the extent feasible.

For more information, call 800-574-5222 to talk with an experienced underwriter or visit banks.progressive.com to view this SafeTalk online.



We know community banks.

Progressive insures over 1,700 banks nationwide. Available coverages include:

Directors & Officers Liability | Employment Practices Liability | Internet Banking Liability | Privacy Liability
Financial Institution Bonds | Excess Deposit Bonds | STAMP Surety Bonds