IDENTITY THEFT AND PRIVACY EXPOSURES

Barry Halpern
Snell & Wilmer

IDENTITY THEFT AND PRIVACY - CLASS ACTION

TARGETS OF OPPORTUNITY

Barry D. Halpern
Snell & Wilmer
April 2007

Recent changes in federal law have given considerable protection to manufacturers and other traditional class action targets. Despite these encouraging developments, nearly every large enterprise faces a new and potentially devastating class action exposure from claims associated with "identity theft" and loss of privacy through unauthorized disclosures of business records. This emerging risk results from an unhappy coalescence of factors, including growing societal interest in privacy, technological developments that facilitate the acquisition and retention of massive amounts of personal information and the class action bar's hunger for new and vulnerable targets.

Identity theft has caught the fancy of the popular media. Horror stories of medical records recovered by dumpster divers, losses of laptop computers laden with sensitive financial information and massive web-based identity scams are raising the visibility of the problem and fueling the public's insistence upon enhanced protection of personal information and privacy. The Identity Theft Resource Center, headquartered in San Diego, estimates that an act of identity theft costs each victim an estimated $800 and 175 hours. The Federal Trade Commission [FTC] estimates that more than 27,000,000 people in the United States were victimized by identity theft between 2000 and 2005, with an accumulated loss of more than $5 billion.

The public's concern, fanned by an ongoing barrage of printed and electronic media stories, largely exceeds the actual risk to victims. Although identity theft can be frustrating, time-consuming and occasionally costly, vigilant consumers have very effective tools to mitigate

and largely avoid significant losses. Delayed recognition is the principal risk to individual and corporate victims of identity theft. When a security compromise is promptly identified, quick action can substantially diminish - and often entirely avoid - the risk of financial loss. By filing "fraud alerts" and notifying banks, credit card companies, and credit bureaus, enhanced credit monitoring can be placed on affected accounts at no charge. These steps substantially limit exposure and free periodic review of individual credit reports provide further protection from loss.

Despite the manageability of the problem, public and enforcement authority concerns have created a fertile environment for imaginative class action lawyers. Over the past several years, the number of highly publicized cases of identity theft has risen steadily, as the "epidemic" has spread to both the public and private sectors. 2006 has been a notable year for identity theft. The United States Department of Defense's loss of an employee's laptop computer containing the personal information on millions of military veterans quickly led to a federal government commitment to pay millions of dollars in credit monitoring expenses. Earlier in the year, the Federal Trade Commission announced that Kansas City's Nation's Holding Company had failed to appropriately protect records with customers' personal information. The agency sanctioned the company, criticizing its policies, procedures, employee screening, training and collection of information. By the summer of 2006, computers with sensitive personal information have become increasingly common. Legislators, regulators and the class action bar have not missed this growing phenomenon.

Concern with the identity theft "crisis" has spawned state and federal legislative efforts to compel prompt disclosure of security breaches. California's 2003 statute requiring notification of California residents when personal financial records are accessed without authority has become a

model for several federal Congressional notification proposals. Although none of the federal bills have passed, various drafts continue to percolate, focusing upon notification, security standards and limits on the dissemination of customer personal and financial information.

As Congress dithers with the issue, the Federal Trade Commission has asserted itself through the enforcement of the Graham-Leach-Bailey Act that requires financial institutions to protect customers' personal financial information. This law requires safeguards to protect sensitive information and advice to the public on encryption and record retention policies. The FTC's enforcement branch has not only aggressively invoked the Graham-Leach-Bailey Act, but asserts independent jurisdiction under the "Unfair Practices" provision of the FTC Act. Operating freely outside the ambit of Graham-Leach-Bailey, the FTC has acted against a wide range of companies that were allegedly negligent in protecting sensitive customer financial information.

Although the law of identity theft remains largely undeveloped and laden with serious challenges to potential claimants, courts and enforcement agencies appear increasingly willing to cobble together creative theories to provide relief to "victims" and growing public interest in "privacy" can be expected to drive politically expedient remedial legislation with potentially devastating consequences to American business.

The fertile opportunity for class action lawyers to assert "intrusion" and breach of privacy claims is equally ominous. That threat will expand rapidly as privacy-reducing technologies become increasingly common in the market and workplace. The use of readily available digital, photographic and satellite-based technologies that allow businesses to acquire and retain enormous quantities of sensitive information on employees and customers will pose a serious liability exposure unless companies develop and enforce rigorous information acquisition and

security controls. As advances in technology race far ahead of the law's capacity to balance the interests of the public, the government and business, the potential for extraordinarily expensive class action litigation will remain a serious challenge demanding careful analysis, security controls and *prompt action* when breaches occur.

1868022.3

Snell & Wilmer
L.L.P.
LAW OFFICES
Character comes through.®

Barry Halpern

Representation in business and health care matters, media law and litigation, including professional liability defense and commercial matters.

PROFESSIONAL RECOGNITION AND AWARDS

The Best Lawyers in America(R), 1991-2007

PROFESSIONAL MEMBERSHIPS AND ACTIVITIES

State Bar of Arizona
Maricopa County Bar Association
American Bar Association
Fellow, Arizona Bar Foundation
University of Kansas School of Law, Board of Governors (1998-2000)
Arizona Association of Defense Counsel
American Academy of Healthcare Attorneys

Partner

Email: bhalpern@swlaw.com
Phone: 602.382.6345

Education

University of Kansas School of Law (J.D., 1973)
University of Kansas (B.A., with honors, 1971)

Court Admissions

Supreme Court of Arizona
Supreme Court of Colorado
Supreme Court of Florida
Supreme Court of Kansas
United States Supreme Court
United States Court of Appeals, Ninth Circuit
United States Court of Appeals, Tenth Circuit
United States District Court, District of Arizona
United States Court of Military Appeals

Location

Phoenix, Arizona

Practice

Bioscience and Health Care
Commercial Litigation
Europe Practice
Health Care Litigation
Health Care Services
Hospitality Services

Publications

Preparing the Physician Defendant in a Medical Malpractice Case

The Wheels of Military Justice the pitfalls of speedy court martial trials

Asset Protection for Arizona Physicians