

## Class Action Privacy Suits: Merchants Beware

Privacy liability is becoming a major exposure and for the moment much of the focus is on credit card information, particularly for legislators and class action lawyers. In the last year one major retailer faced more than 20 suits and a multimillion-dollar settlement following the theft of more than 46 million credit card numbers. These suits and other factors such as the increasing use of recent federal legislation known as FACTA as a basis for consumer class actions are magnifying the risk. State legislators are also involved. Breach-notification statutes have been passed in 37 states (so far) and we are now seeing in Minnesota (a key state for many credit card companies) the beginnings of what might be a trend: financial responsibility for credit card security breaches has been shifted to merchants on a strict liability basis.

Because Congress seems unable to develop a national notification standard, a confusing matrix of state laws will continue to provide the authority over the credit card privacy issue. The following is an update on this developing and potentially expensive exposure.

### The FACTA Factor

In 2003, Congress tried to set the tone when it passed the Fair and Accurate Credit Transactions Act (FACTA) requiring that "no person that accepts credit cards or debit cards...shall print more than the last 5 digits of the card number or the expiration date upon any receipt..." Since its enactment, *more than 100 class action lawsuits* have been filed in California federal courts alone alleging violations of the statute.

While on its face FACTA seems fairly clear, lawyers have found wiggle room in an apparent ambiguity in the statute, which may arguably require either: (1) **both** the truncation of the numbers **and** the deletion of the expiration date, or (2) **either** the truncation of the numbers **or** the deletion of the expiration date. While cases are being filed, almost as we speak, there is still no clear-cut guidance on even this simple point.

For a willful FACTA violation, which sometimes requires only "reckless disregard," the law authorizes damages of \$100 to \$1,000 per violation, without proof of actual injury. As each receipt can be a violation, the math is simple. For a company that processes 20 million credit card transactions per year, the penalty could amount to \$2 billion each year, plus attorney's fees and costs.



### Is Liability Passing to Merchants?

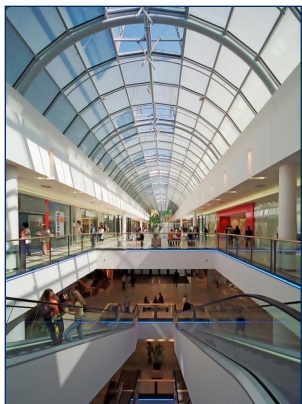
In May of this year, Minnesota passed legislation that makes retailers and other merchants liable to banks for costs associated with data breaches. The measure prohibits merchants from retaining information drawn from the magnetic stripe of a credit or debit card and the personal identification number (PIN) or access code after completion of a credit or debit card transaction for longer than 48 hours.

The legislation permits banks to sue the relevant retailer(s) for "the cost of reasonable actions undertaken" to respond to a breach, including the costs of cancelling and reissuing credit cards, closing and/or reopening accounts, stop-payment actions, unauthorized transaction reimbursements, and providing breach notification to cardholders. As long as a "person or entity" conducts business in Minnesota and accepts "a card containing magnetic stripe data or a processor chip" in connection with a transaction, that person or entity becomes

automatically liable to any "financial institution" for the "reasonable costs" undertaken to protect the information of its cardholders.

Complicating matters, the bill doesn't specify that the merchant needs to be headquartered in Minnesota, that the breach has to have happened in Minnesota, or that the financial institution has to be located in Minnesota. While the new law applies to data breaches occurring after August 1, 2008, banks are already beginning to seek redress from merchants. At least four other states – Connecticut, Illinois, Massachusetts and Texas – have similar legislation pending.

## Liability for Costs of Fraud



Merchants seem unable to get a break from any quarter. A US district court recently joined the fray by allowing banks to continue seeking damages for the losses arising from the theft of credit card data from a large retailer. The losses, which have been estimated at between \$68 and \$83 million in this case, were previously thought to rest with the banks as they had

no direct contractual relationship with the merchants who lost the information. The court, however, managed to get around the lack of a contractual relationship by ruling that the merchants could be liable because they knew that the banks issuing the credit cards were part of the financial network that relies on its members taking "appropriate security measures."

## Insurance to the Rescue?

Where can merchants turn for protection? The first logical place to look for coverage for liability from loss or theft of credit card information is under the Personal Liability section of the ISO Comprehensive General Liability (CGL) form. However, since a CGL policy requires "publishing" of the credit card information in order to trigger coverage, and publication is usually *not* an element of these cases, there may be little or no coverage to be found here.

The next logical place to seek insurance is under a Professional Liability or Errors & Omissions (E&O) policy. Unfortunately, merchants typically do not purchase Professional Liability coverage; even if they do, credit card information liabilities usually fall outside the definition of professional liability found in those policies. Another dead end.

Coverage is available, however. Extended forms of Privacy and Network Security coverage (sometimes known as Cyber or

Cyber Liability coverage) can provide protection against liabilities arising from this new legislation. Coverage can be purchased for events related to computer systems (and other systems) as well as for the vicarious liability from disclosures by vendors or service providers holding credit card information on a company's behalf. Furthermore, these policies can be extended to cover notification costs required by state laws and costs of credit monitoring that must often be provided to affected credit card holders. Recently, insurers have added coverage for regulatory defense costs and for fines and penalties arising from certain statutes (where such insurance is allowed by law).

As the risks associated with privacy liability evolve, so will the insurance products that address them. And along the way, the risk manager's job will grow ever more complex.

## Executive Risks Regional Contacts

### Atlanta, GA

Charles Maxell  
P- 404 224 5123  
F- 404 224 5001  
charles.maxell@willis.com

### New York, NY

Steve Pincus  
P- 212 915 7940  
F- 212 519 5460  
steve.pincus@willis.com

### Boston, MA

David Goldstein  
P- 617 351 7498  
F- 617 351 7430  
david.goldstein@willis.com

### Radnor, PA

Matt Schott  
P- 610 254 5642  
F- 610 254 5600  
matt.schott@willis.com

### Chicago, IL

Brian Gauen  
P- 312 621 4855  
F- 312 621 6870  
brian.gauen@willis.com

### San Francisco, CA

Michael Mahoney  
P- 415 291 1535  
F- 415 982 7978  
mike.mahoney@willis.com

### Denver, CO

Jim Iacino  
P- 303 218 4039  
F- 303 218 4058  
jim.iacino@willis.com

### Toronto, ON

Jonathan Ashall  
P- 416 646 8351  
F- 416 869 1649  
jonathan.ashall@willis.com

### Los Angeles, CA

Chris Crawford  
P- 213 607 6294  
F- 213 607 6301  
chris.crawford@willis.com

Executive Risks Alerts and Newsletters provide a general overview and discussion on a wide range of topics. They are not intended, and should not be used, as a substitute for legal advice in any specific situation.