

April 23, 2008

Companies May Be Held Liable for Deals With Terrorists, ID Thieves

New and little-known regulations could mean fines, or even jail time, for companies that do business with bad guys.

OK, pop quiz. A local car dealership sells a car to a new customer. A week later, that same automobile is used in a terrorist car bombing. The business can't be held liable for what the customer did, right?

Wrong, according to several U.S. law enforcement agencies. In fact, if your company provides products or services to a terrorist or identity thief, it may face six-figure fines -- or even jail time for its officers.

"With all of the focus put on compliance and security breaches, it's easy to overlook these requirements around identity and law enforcement," notes Brian Bradley, executive vice president of strategy and emerging markets at MicroBilt, which vets customers and trading partners on behalf of its small-business clients. "It's another level of compliance that a lot of companies don't even know about."

If you're a security pro, you might be familiar with the U.S. Treasury Department's Office of Foreign Asset Control (OFAC) requirements, which basically require companies to check their customers' identities against a list of known terrorists to prevent them from unwittingly providing products or services to an enemy. Most major credit bureaus check customers and applicants against these lists, so if you're vetting your partners and customers that way, you're probably covered.

However, you may not have heard yet about the Federal Trade Commission's "Red Flag" program, which is designed to warn companies when they are about to do business with identity thieves or money-laundering operations. The Red Flag program, which takes effect Nov. 1, requires enterprises to check their customers and suppliers against databases of known online criminals -- much like what OFAC does with terrorists -- and also carries potential fines and penalties for businesses that don't do their due diligence before making a major transaction.

"The final rules require each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program for combating identity theft in connection with new and existing accounts," the FTC says in the rules, which were passed last year.

"The Red Flag rules are basically there to help protect consumers from identity fraud, and to help prevent businesses from making bad loans or extending credit to criminals," Bradley says. "But a lot of security people don't know much about them yet, and most small businesses -- the ones that are too small to work with the big credit bureaus -- don't know anything."

However, many organized terrorists and criminals know that small businesses can't afford to work with the big credit bureaus, which makes these mom-and-pop shops prime targets for illegal purchases and money-laundering scams, Bradley observes.

Story continues...



April 23, 2008

"And the worst part is that the small business can be held liable if it does do business with the bad guys, even if it isn't aware of the regulations. I haven't seen any cases yet, but the Red Flag rules won't be enforced until November, so we're just beginning to deal with those."

MicroBilt is out spreading the word on these emerging regulations because next week it will unveil a new service offering that helps small businesses vet their customers, suppliers, and even employees to comply with the OFAC and FTC Red Flag rules.

As part of its regular "risk management" service, which provides screening, tracing, and identity and background checks on potential clients or trading partners, MicroBilt will now offer a "watch list" service that checks these individuals against 63 different lists from 35 sources, including OFAC, the FBI, and Interpol, Bradley says.

"It's an easy way to be sure you're not dealing with someone you'll regret later," he says. "And it's also a way to be sure you're in compliance with the emerging regulations and databases, which are too complicated for most small businesses to deal with."

The watch list service is free with the MicroBilt service, which is sold on a per-transaction basis and includes vetting of any individual -- customers, potential employees, or even principals at prospective suppliers or trading partners. Microbilt will even guarantee the transactions of individuals vetted through its service, Bradley says.

"Any business that's in the chain of private consumer data should be thinking about these [regulations]," he says. "You need to be able to detect if you're dealing with a suspicious character, both from a business standpoint and, increasingly, from a legal standpoint."

