

U.S. 'red flag' rules could affect Canadian banks

Nov. 1 has become a deadline for financial institutions south of the border to comply with regulations that might reduce the threat of identity theft. Entrust offers tools to make the grade

BY KATHLEEN LAU

A new regulation requiring banks and creditors to identify potential consumer identity theft is scheduled to take effect in the United States on Nov. 1, but at least one industry expert said Canada could also experience the spillover effects.

The regulations under the Fair and Accurate Credit Transactions Act (FACTA) require that institutions implement programs to seek patterns in consumer and employee behaviour that might indicate possible foul play. Any organization involved in credit decisions are affected by the regulations, known as the "red flag" rules.

But while only U.S. banks and creditors must comply by Nov. 1, Adel Melek, partner and global leader of security and privacy services with Toronto-based professional services firm Deloitte, said he thinks the regulation could eventually spawn a Canadian version. "Invariably every time there is a piece of legislation that gets introduced, especially in the U.S., there is some consideration for its application in Canada," said Melek.

He did however add that it would likely take the form of a guideline, rather than a regulation, as has typically been the case north of the border, and "in Canada, by virtue of having a guideline, there would by default not be clear consequences or claws or teeth."

But besides a Canadian version of the red flag rules, Canadian banks expanding services south of the border will either have to figure out how to earmark U.S. customers (based on identifiers like address or citizenship) in order to ensure compliancy, Melek said, or extend blanket coverage.

According to Danny Shaw, global practice leader of technology risk management with

U.S.-based Jefferson Wells, the new regulations stem from the fact that identity theft criminals were taking advantage of gaps in existing U.S. legislation like with the Fair Credit Reporting Act founded in the 70s. "So if you think of it, this is really an identity theft regulation even if they're calling it the red flag rule," he said.

An instance of a red flag might be when a customer's identity, such as an address or social security number, is not encrypted and readily accessible on documents or computer systems.

The regulation's area of coverage is broad, encompassing approximately two million organizations. And, the requirements will affect people, processes and technology that might be in place to manage credit decisions, said Shaw, meaning the impact could potentially be quite "huge" for some organizations.

But while those institutions were made aware of the looming deadline early this year, a recent BankInfoSecurity survey found that almost half of 300 surveyed institutions will either barely meet or will miss the deadline.

Lack of awareness is a contributing factor, said Shaw, but time constraints and the number of regulations that a business must comply with can often complicate the matter. "They need to look at this as part of their normal best practice... While you're doing these other things, you need to do this also," said Shaw.

And compliance is crucial, he said, citing the identity theft incident that cost retailer T.J. Maxx an approximate US\$4.5 to 8.6 billion in damages. "We're talking real money there," he said. "This is not one of those things where we lost someone's record [and] we'll send them a sorry letter. This is

true loss of dollars if they don't get this done."

Shaw said institutions should perform a risk assessment, then identify controls to mitigate that risk, and finally get a third-party company to review the program. And, he added, that while it is primarily the responsibility of the compliance or audit department to ensure compliancy, IT also has a role to play.

One Ottawa-based company of layered security technology is promoting two products as systems that can help institutions facilitate compliance with the red flag rules. Product manager with Entrust, Mike Moir, said one of the products, IdentityGuard, provides second-factor authentication to meet the varying skillset of the consumer market.

The other, TransactionGuard, monitors all customer transactions to identify red flag behaviour. Certain transactions in isolation won't signal foul play, but Moir said "in combination, then that increases a risk or enough that it can trigger an action to take place." The system comes equipped with a repertoire of red flags, but IT administrators can augment that with their own.

Although it's great to have the tools in place, Moir said that processes are also important. The company has a professional services department to aid with process implementation, he said.

Moir said that financial institutions, particularly in the last several years, have been curious around authentication technologies. But while the interest stems primarily from U.S.-based banks, Canadian banks, too, have shown that they "are very progressive and are always concerned about customer information."

As for the effectiveness of the regulation, "the proof is going to be in the pudding when this gets rolled out," said Melek, adding that success can then be measured by whether there's an observed reduction in identity theft incidents.

To find similar articles visit www.itworldcanada.com