

Limit ID Fraud: Use Identity Scoring, Not Credit Monitoring

Avivah Litan

Enterprises that are targets of data breaches or other types of data compromise almost universally offer free credit report monitoring to potential victims. However, these services are limited in the type of protection they offer. Newly emerging identity scoring and monitoring services offer more protection but are still immature and not widely adopted. Both types of services have their limitations in the kinds of frauds they can detect.

Key Findings

- Identity theft fraud prevention and detection services fall into two complementary components: services sold to enterprises and services offered to consumers, either directly or through breached enterprises.
- Services available to consumers include credit report monitoring or identity monitoring.
- Credit report monitoring watches consumer credit reports and associated activities that feed into the consumer's credit score, which measures their creditworthiness. Identity monitoring watches a wider set of consumer data, including credit reports, that feeds into a consumer's identity score that gauges their legitimacy.
- Credit report monitoring is not as effective as identity scoring when it comes to detecting new account fraud.
- Neither identity scoring nor credit report monitoring can catch many types of frauds perpetrated on identity theft victims.
- Identity scoring is an emerging application and is not widely offered or used. For now, it is generally available to enterprises for scoring the fraud risk of an identity when granting new credit or opening new accounts. Direct-to-consumer identity scoring and monitoring services are limited but are growing.

Predictions

- Identity scoring available directly to consumers will overtake credit report monitoring as an effective identity theft prevention tool by year-end 2009 (0.6 probability).
- Other, more-comprehensive identity-theft-related fraud detection services that look at types of fraud besides new account fraud — such as account takeover or misdirected benefit or claim payments — will be offered directly to consumers by year-end 2009 (0.7 probability).

Recommendations

- If your enterprise has suffered a data compromise, provide your customers with identity scoring services instead of or in addition to credit report monitoring. Some services are directly available to consumers, and these will become more widespread by the end of 2006.
- More commonly available are identity scoring services sold to enterprises that use them on the back end. An individual's record can be scored for fraud risk using these back-end services, so breached enterprises can continually monitor the risk faced by potential victims by scoring their risk of identity theft fraud.
- Continue to offer potential victims credit report monitoring as a secondary option but be sure to educate your customers on the shortcomings of both credit report monitoring and identity scoring.

ANALYSIS

Stolen laptops containing sensitive customer and/or employee information are almost a daily occurrence. More-serious data breaches and criminal accesses are also taking place at retailers, payment processors and other types of companies. Following a compromise, affected enterprises — including government agencies and private-sector companies — almost universally offer potential victims free credit report monitoring from one of three U.S. credit bureaus: Experian, Equifax or TransUnion. While this offer is better than nothing, it implies that credit report monitoring will protect customers from criminal use of their identity records for subsequent crimes.

The suggestion that credit monitoring will protect customers from future fraud is simply a gross misperception. Interestingly, most affected consumers are not signing up for free credit report monitoring offered in response to a breach. Perhaps that's because U.S. citizens are already entitled to three free credit reports a year (or one from each of the three bureaus). Or perhaps individuals understand credit report monitoring doesn't buy them the implied assurances. Even more probable, consumers don't understand what credit report monitoring does for them in the first place.

Why Is Credit Report Monitoring Deficient?

Credit report monitoring has two main deficiencies:

- First, it will tell a potential victim only if his or her exact identity (matching Social Security number [SSN], name, date of birth [DOB] and so on) was used to apply for a new credit card, mortgage or other type of loan, or if there was a late payment or other account activity that is reported to the credit bureaus (for example, closing of an account, a change of address, a credit inquiry). It will not report such activities to a victim whose stolen SSN is used in conjunction with other data that does not belong to the victim, such as a modified address, DOB or name.
- Second, a credit report monitoring alert comes days *after* the potentially criminal activity — it is not proactive, so it only enables the victim to start the fraud-reporting process faster, hopefully before too much damage is done.

What Is a Better Alternative?

Identity scoring and monitoring is more effective than using credit report monitoring to watch for potentially fraudulent activity. That's to be expected. Identity scoring and monitoring was explicitly architected to look for identity-theft-related fraud. Credit scores were designed to help lenders make good credit decisions. Direct-to-consumer credit reports and monitoring evolved several years ago when consumers wanted to know the content of their credit score. Consumer credit report monitoring further developed as a way for consumers to directly monitor inquiries about their credit reports to determine if such inquiries were made for either legitimate or potentially criminal purposes.

Identity scoring and monitoring — an emerging application available from only a few vendors in the anti-fraud business — scores and monitors events *before* credit is granted or a new account is opened. It is much more effective in identifying new account fraud than is credit report monitoring because:

- It doesn't rely on a match of SSN and other attributes — such as name, address and DOB. Therefore, unlike credit report monitoring, it can catch:

- Uses of an SSN attached to variations of the existing name, address, DOB and/or phone number, and so on that belong with it.
- Uses of an SSN attached to an entirely new, fictitious identity that appears legitimate over time. For example, an identity thief will manage to establish various accounts (cellular phones, credit cards and bank accounts) over time and will initially pay bills on time so that the identity continues to appear legitimate. Later on, the thief will use the fictitious identity to steal money out of the system; for example, by not paying bills, taking large cash advances and engaging in other fraudulent activity.
- Identity scoring scores the "behavior" of an identity's or a criminal ring's activities over time and across enterprises. Suspect patterns of behavior that show up across different organizations would not necessarily appear if the activity within only one organization was being monitored. Credit report monitoring does not do this and does not purposefully detect activity of criminal rings or individual records that are linked through the use of stolen or "fictitious identity" data.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509