Fraud Just Ain't What it Used to Be

21 February 2013 By: Al Pascual

The good old days when the bad guy had to get a bit dirty to steal your personal info have come and gone. The anonymity and convenience afforded to today’s digital crooks has prompted a paradigm shift in the way that fraudsters do business to the detriment of consumers, merchants, and the financial industry. Data breaches are a considerable driver of fraud according to Javelin’s 2013 ID Fraud Report, as nearly 1 in 4 consumers who were notified that their PII had been compromised in a breach later suffered from identity fraud. On top of breaches is an epidemic of malware that has begun to infect mobile devices, where Zeus, Citadel, and SpyEye have mutated to become Zitmo, CitMo, and SpitMo – while not the cleverest of nomenclature adaptations, they certainly make dumpster diving and mail theft look quaint by comparison.

It’s not just the means by which PII is compromised that has gone high-tech, as a victim’s information is used to make a purchase online in 45% of all identity fraud cases in 2012 (up from 41% last year). Fraudulent purchases at the point of sale (35%), unauthorized ATM withdrawals (6%), and phony checks (5%) are all losing steam – having to commit fraud in person has fallen out of favor. Recognizing your enemy’s capabilities is necessary for an effective defense – fraudsters have figured out how to steal voluminous amounts of PII, and either sell it or use it to commit fraud in a way that doesn’t require them to leave their couch. Install anti-malware, actively monitor your accounts, demand strong authentication, consider identity protection services, encrypt everything – common sense is still an important tool, but if the bad guys are going to level up, then so should we.