March 3, 2013 - If you still believe identity theft is a marketing gimmick, it's time to take a look at the Federal Trade Commission report released this week. Identity theft is once again the top complaint in America, as it has been for 13 years. Identity theft complaints surged by 32 percent in 2012 to nearly 370,000, and that number is intensified by the most recent Javelin report, which puts the number of instances of identity theft at 12.6 million. Even Javelin's figure is probably way lower than the real number, when you factor in all the cases that go unreported or categorized improperly.

It is no longer a question of if your identity will be stolen -- the only unknown is when it will happen. The same goes for companies and government agencies that gather personal data on employees and consumers: there will be a data breach.

Hackers, identity thieves and fraudsters of all stripes have reached the conclusion that a stolen identity is a key that can unlock all kinds of fraud: opening doors to millions of dollars in instant profit, services and/or treatments on someone else's dime, even offering up an innocent fall guy to law enforcement officials all too eager to "get their man." Even if criminals weren't relentlessly hunting for our personal information (which they are), the steady stream of massive data breaches at companies and government agencies from the Department of Veterans Affairs to Blue Cross Blue Shield to the U.S. Environmental Protection Agency to the South Carolina Department of Revenue to Sony to Twitter to LinkedIn (to name a few) guarantee that at least some, if not all, of your personal identifying information has already been exposed to folks who know how to take the particulars of your life to promote their welfare.

The largest area of growth in the FTC report by a mile has to do with tax returns. Identity thieves have clearly developed a preference for this low-hanging fruit, and the closely related practice of using someone else's Social Security number to apply for a job (and sticking the victim with the tax bill). In 2010, only 15 percent of identity theft cases involved tax or wage fraud, which was more or less even with credit card, phone and utilities fraud.

According to the FTC, identity theft was the most common type of crime reported to them last year, accounting for 18 percent of all complaints, nearly twice as many as the next category -- debt collection -- and significantly higher than in 2011, when identity theft accounted for 15 percent of consumer complaints.

After two years of solid increases, however, last year tax- and wage-related fraud accounted for an astounding 43 percent of all identity theft complaints. Compared to other types of identity fraud, it wasn't even a contest. The next most common complaint was credit card fraud, which accounted for some 13 percent of reported crimes.

What is going on here? It's hard to say for sure, but Florida is illustrative of the problem. For years, the Sunshine State has hovered around the five spot in the top 10 list of states with the worst identity theft epidemics.
La
st year Florida blew all the other states away. About 360 Floridians per 100,000 reported ID theft to the FTC last year, nearly twice the rate of runner-up Georgia and three times greater than California, which came in third. The complaint rate in Florida in 2012 was more than twice what it was just a year before.

When you break the numbers down by metropolitan statistical area (MSA), Florida's quandary grows even worse. In 2012, it was home to nine of the top 10 MSAs in America with the highest rates of identity theft complaints. No state has ever dominated that list so completely.

That's not a trend. It's an epidemic of epic proportions. And nearly three-quarters of all identities stolen in Florida were used to commit government documents or benefits fraud. That category includes a broad sweep of crime, including stolen tax refunds, stolen government benefits, and stolen or invented government-issued IDs, which enabled imposters to gain employment.

Based on the FTC's report, it's impossible to fully explain this sudden surge in Florida's overwhelming exposure to government documents fraud. Are countless undocumented workers using stolen IDs to apply for jobs? Are retirees suddenly re-entering the workforce in droves and applying for refunds? Has a crime syndicate discovered the next best thing? Your guess is as good as mine.

Given the inevitability of victimization, the only way to protect yourself is to prepare for identity theft in the same way you would death, taxes and the sequestration. Identity theft has become a rite of passage. It's one of the true certainties of life nowadays. Your identity will be stolen. Your employer will be hacked. Your organization will experience some form of database compromise that will put its reputation, customers and employees at risk.

If you are a consumer, you must minimize your risk of exposure, do whatever is necessary to detect victimization (and your credit score, if you check it regularly, can be an initial indicator that something's gone horribly wrong) and put a damage control program in place.

The same goes for institutions. If you gather Personally Identifying Information (PII) on consumers, taxpayers or clients, someday you will lose it, either through a malicious hack or due to human error. To better protect your organization: encrypt the data you collect and store, install the latest security software (and frequently update it), lock down your physical security, restrict computer access to only those who need it, continuously train and test your employees and rigorously screen all job applicants. (Note to HR departments: Don't demand Facebook user ID and password information. There's ultimately no upside to it and you could put yourself in the crosshairs of a regulator or class-action attorney.) Also, demand all of the above of your vendors.

Final note: When (not if) your systems are breached, you'll need to know the rules for breach notification in all the states where you operate (a word of warning: no two states are necessarily the same) and implement a breach response program. Notifying your victims will take money, and so will the lawyers you'll need to defend the organization from increasingly likely legal action. Have you secured the proper insurance coverage? Do you have a contingency for this in your annual budget? Failure to do this might well represent a violation of your fiduciary duty to customers, employees, partners and investors and ensure a major strike against you when regulators come knocking at your door.

Here's the reality, and this is not a simple scare tactic: At some point an identity thief is going to get you. When your identity is stolen or your organization is compromised, it's vital that you are ready for it. The time to prepare is now. Actually, it was yesterday.

Adam Levin is the former director of the New Jersey Division of Consumer Affairs which gives him unique insight into consumer privacy, legislation and financial advocacy. He is a nationally recognized expert on identity theft and credit.