Comments

Of

Michael Stanfield, CEO, Intersections Inc.

At

THE PRIVACY SYMPOSIUM – SUMMER 2008:

PRIVACY IN TRANSITION

An Executive Education Program on Privacy and Data Security Policy and Practice

August 18 – 21, 2008

Harvard University, Cambridge, MA

Symposium Hotel: Charles Hotel

.

Let me start by thanking each of you for the opportunity to address an area that concerns all of us in the arena of privacy and identity management.

I would like to take a few minutes to discuss a few concepts, some of which have already had air time at this conference, and conclude with an appeal for cooperation between the identity management industry and you as members of the privacy advocacy, privacy legislative agenda and business privacy management leadership communities.

Despite all the concern, efforts and work put forth by government, the legal and academic industries, and by consumer protection advocates – American consumers have demonstrated time and time again that while they desire privacy that desire is often overshadowed by other more seemingly important objectives. Since privacy laws are predicated on consumers' proactivity – typically opt in, consumers need a better understanding and useful tools and incentives to increase their proactivity towards privacy protection.

In a recent survey by AOL, 84% of participants responded that they never give out personal information online, yet AOL research reveals that 89% of all Internet users have freely shared personal information online.

Consumers are driven by economics and the need for social contact. In this context, they do not seek privacy; they seek monetary flexibility, economic reward, and social interaction. These needs are not tempered by knowledge of the associated risks, but rather are stimulated by misinformation.

Even in this bad economy, credit card offers continue to flood mail boxes for one reason - they work.

In-store discounts drive credit card account openings for one reason – they work.

Classmates, FaceBook, LinkedIn and other social networking sites have grown and continue to grow at incredible rates despite often reasonable, but under utilized security. These new institutions stimulate the development of online socialization; but they also inadvertently create a lowering of the guard of an entire generation of future consumers with a propensity to conduct commerce online.

Online registration in exchange for a free service or offer at discount creates incremental margins for online merchants who then sell unaffiliated products after selling their own products. These offers work because so many people are willing to give up information to companies they do not know because they get something they perceive to be of economic value.

At the end of December 2007, there were approximately 112 million blogs and growing at a rate of 175,000 new blogs per day. While many foster valuable information flow, many are like airplanes, someone you don't know and don't really want to know, snuggling up to you and telling you their life story while you are trying to read a good book.

And to illustrate the issue of American consumers and the almighty dollar just look at how low the war in Iraq ranks in importance compared to economic issues in current political polls.

In conjunction with seeking economic reward and social interaction, consumers have demonstrated complacency with respect to their engagement in the management of their privacy and identity. Consumer inactivity in this management process is driven not only by the need for social interaction and the desire for economic action, it is also driven by misinformation. Which leads me to my next point – misinformation.

Consumers are told by some consumer advocates:

"You do not need to buy monitoring services; you just need to look at your free credit report."

Consumers are told by some companies that consider themselves in the identity protection industry that they just need to put a fraud alert on their credit file or just monitor their credit file to prevent identity theft. When we started working with one of the credit bureaus to create the first daily monitoring product using their skip-trace process as the backbone of the product, daily credit monitoring became an effective method of detecting financial fraud, but credit monitoring was neither designed nor intended as a preventative solution – despite the advertising copy of some in our industry. However, in the late 90s, it was the best and only tool to detect financial identity related fraud. Today, we have better preventative tools.

Last year a large Internet service provider advertised that if you used its service, identity theft was "zapped".

TJ Maxx currently has an FAQ on their website that states:
Am I at risk for identity theft?

Experts tell us that it would be extremely unlikely for cyber thieves to commit identity fraud with the vast majority of information that we believe was stolen. This copy remains on their website despite the recent disclosures.

Many financial institutions struggle with the losses related to account takeover and other identity related fraud and continue to pay as the numbers and size of the problem grow.

Institutions are focused, but have a hard time dealing with the need for improved authentication and identity verification processes due to a concern that the complacent consumer will impatiently move their business to the institution next door which has easier faster access – albeit far less secure access. This was a recurring theme two years ago when we and a major consulting firm approached a group of institutions with some new technology and business process ideas to reduce account takeover risks.

David Einstein of the San Francisco Chronicle, in an online article this past Monday while answering the question whether consumers should sign up for an identity protection program, wrote "no, no, no, and a thousand times no" and continued
"The odds of having your identity stolen online are lower than the odds of Keanu Reeves winning an Oscar. Online banks and stores encrypt credit card numbers and other personal data transmitted over the Internet, so your identity can't be stolen."…Mr. Einstein apparently doesn't understand keylogging, phishing or sniffing. Interestingly, a recent study calculated 1.5 million identity thefts in California and California is rated 1st in work related identity fraud.

We all have contributed to the consumer's confusion with respect to privacy, identity theft and identity management. The consumer is misinformed that it's not that big a problem or it's somebody else's problem or it's easy to manage – or all 3.

Accordingly, we leave the consumer to deal blissfully in a widening valley of fraud plying the consumer's desire for economic action and social interaction while thieves see this valley as a valley of low hanging fruit.

So what is at the end of the valley of fraud?

In the government and regulatory sector work continues, and over time more rules will be enhanced, regulations will be advanced, and legislation will be pressed.

In the business sector there will be growing competition, and there will be progress, but there is no sight set on unified or federated multi-factor identity verification processes and therefore the problems will not go away.

And as major corporations, government, and interest groups rightfully debate, negotiate, regulate and legislate, consumers and businesses will continue to loose billions of dollars, costs will continue to rise higher than necessary because the Internet is not maximized as a vehicle for commerce, and many consumers will be faced with the reality that identity fraud is far more pervasive than having money illegally taken from their account and asking their financial institution to refund their losses. It can and does disrupt lives and often creates emotional strain.

Identity related crimes will cause other issues for consumers.

Some examples from a few of our customers:

- **Kevin sought a job a few months ago as a young radio announcer, he won the job in this high speed competitive industry that is hard to break into. Background check – a criminal record was recorded against his SSN, and the job was lost to another candidate while he was trying to clear his name. Reviewing or monitoring his public record information would have prevented this. Whether or not clerical error or identity theft was important to Kevin, the impact it had on his life was important**

- **John sought a coop in NYC. Goes to closing, and the bank does a preclosing credit review. Two new loans in the past thirty days, and three new credit cards in past thirty days. The bank refuses to fund John. John loses the coop to another bidder while clearing his files. John is not responsible for the bad accounts, but John lost the apartment of his dream and goes back into the market place.**

- **We have all read stories of illegal immigrants using someone else's SSN, then not paying taxes, then the real consumer gets a call from the IRS. Who wants or needs a series of calls from the IRS, putting the burden or proof on the innocent consumer?**

- **Now the criminals don't work, they file for refunds in the name of people that work for them.**

You all have read the new TJ Maxx indictments. Why are we surprised? Identity fraud, account takeover, these are sophisticated crimes and they will find it tough to prosecute the unidentified co-conspirators. This breach exemplifies the tip of the iceberg of the accounts illegally taken from files and computers in the last few years. How many seeds of identity related financial fraud are sitting in the farm servers of criminals building synthetic IDs or mining for incremental information and phishing and keylogging to create opportunities for account or identity takeover in anticipation of future use of an innocent persons information or bank accounts?

And within this backdrop, institutions often provide six or twelve months credit monitoring to protect a consumer after a security incident. The problem is that harm may not come in six or 12 months. It can come far down the road – well after 12 months, and it cannot be stopped by looking at a credit report today or in six months. Breach mitigation services need enhancement of product and duration to become effective.

However, at the same time, the press needs to learn to distinguish between the theft of a useable and meaningful PI file and the inadvertent loss of an unusable and strongly encrypted file.

I opened by saying I wanted to conclude with an appeal for cooperation.

For all the hard work to create safe physical banks, safe cars, and safe homes, we are still in a community of risks. While laws are passed to protect us, and while police roam the streets, and while insurance companies protect our losses, we are still vulnerable. We install locks, we lock gates, we live in gated communities, we install alarm systems, and we die in traffic accidents. The individual has a responsibility to himself or herself over and above the responsibility of the state or society.

Today there is a popular view that protecting our privacy and our identity management is a matter of responsibility and management among institutions, government and business. I submit to you that that is only part of the answer. Consumers need to be more educated, more responsible, and move from complacency to vigilance in the nonphysical world just as we have evolved to secure ourselves in the physical world notwithstanding the protections afforded by government. To prevent fraud, consumers must be vigilant. But first they need to understand the risk – the risk of going online at an airport, the risk of keylogging, the risk of swiping a card in the wrong place, the risk of giving out credit card information to unknown merchants or via a cell phone in an airport lounge. The list of risks goes on and on and gets more complex each day as criminals write another sinister code applet, sit in public areas sniffing computers or record a series of conversations using listening devices. Once educated, most consumers will become vigilant and use security tools to manage their computer, phone and internet activities, vigilant to decide when and how to use their credit cards, vigilant to gauge when they provide access to their

personal information, and vigilant to monitor their financial and sensitive personal records in a timely manner so they can catch the thief before the financial fraud disrupts the consumer's life. We all need to work together to educate our consumer constituents of the risk and the need for vigilance.

How do we reduce the risks?

Clearly your efforts on the privacy front to guide business practices and push on the legislative front will help.

And the financial and merchant industry will become more vigilant at their gates over time.

And the consumer protection industry needs to continue to evolve to create products that educate consumers and prevent identity frauds, and law enforcement and regulators need to deal with those that purport to be in our industry and that prey on fear with false and deceptive promises, meaningless million dollar guarantees and useless products. Consumer protection services need to meet four criteria:

- **Educate the consumer**
- **Prevent identity theft**
- **Detect identity theft if it occurs, and**
- **Resolve identity theft quickly and thoroughly when it occurs.**

Creating highly sophisticated preventative services is our goal, and should be the goal of all in our industry. If we succeed consumers will be educated and more protected and we will all be better off in the long run.

There is no simple answer, and we need your help and understanding that in my industry there are those that make bona fide efforts to create services that actually help, and there are those that take short cuts primarily relying on advertising, sometimes deceptive, without substantive services.

I urge you to understand the difference, and to not put us all in the same basket.

Thank you very much for listening.