

AMERICA'S LEADING IDENTITY RESOLUTION AND EDUCATION SERVICE

THIS MONTH'S TOPIC...

2010: **Accountability** 2.0

Are we ready to face a new decade?

It's not just a new year, but a new decade. Yet, as we celebrate our recently passed milestone, the challenge of dealing with old problems — identity theft, consumer fraud, organizational data breaches — remains.

The changes needed in the government, business and consumer sectors require a long-reaching impact. The digital era is still young, but in this new decade it will mature. It is everyone's responsibility to ensure that personal privacy and identity protection are embedded into its evolution.

In this month's newsletter, we look back at 2009's identity theft failures, lessons and triumphs, with an eye toward foundational changes that might have a positive, long-term effect on the future. We recognize that the online world is largely uncharted territory and that the best practices we can identify and apply here—on all levels—can help put us on a path to a more secure future.

Here's to where we've been ... and to where we need to be.

For a complete newsletter archive, visit: www.identitytheft911.org/newsletters

To learn about the latest scams on identity theft, visit: www.identitytheft911.org

Comments, questions? Contact us: newsletter@identitytheft911.com





University of North Carolina at Chapel Hill

2009

The Year in Identity Theft

Large Data Breaches, a Big Bust and Huge Potential for Change

Everything related to identity theft in 2009 was big. Big data breaches. Big arrests. Big new problems affected one of the biggest jobs Web sites on the Internet, and a big, embarrassing security debacle involving the president's private helicopter details.

Even long-standing issues stayed big. Many federal agencies, including the departments of Defense and Energy, still had holes in their computer security systems that posed a threat to national security. Congress and the Federal Trade Commission failed — four times — to enforce new regulations that could protect consumers from identity theft. In all, we saw vulnerabilities (and a few victories) across government, business and consumer sectors. Granted, some lessons have been learned and some progress has been made, but we need great strides. The paradigm shift toward true accountability in the consumer, government and private sectors won't happen without concerted effort from all parties.

All of this means that we still have serious work ahead of us for 2010. In the bird's-eye view, this means that government needs to do more to protect consumers from hackers and identity thieves by creating, implementing and enforcing consumer-oriented legislation. The private sector must guard consumers' sensitive personal and financial data, and not issue credit to impostors. Consumers must monitor their credit and accounts, and keep their own sensitive information under lock and key (digitally and in hard copy) — not to mention exercise restraint in their online activities, whether it's shopping or social networking.

Past experience, however, is an excellent tool for determining how we can all improve. And many of 2009's top stories illustrate where all sectors can step up their accountability. ►

Data breaches go big-time

The total number of data breaches reported in the U.S. might seem to belie the notion that 2009 was another big year for data breaches and identity theft. According to the Identity Theft Resource Center, there were 240 data breaches from the start of 2009 and on Dec. 10, the last date for which information is available. There were 307 breaches by this time in 2008. That represents a significant drop in the number of reported security breaches in just one year.

That drop comes with two caveats, however. First, it's important to remember that the resource center only tallies breaches that are reported. Since

Either way, this highlights the fact that many data-keepers (business and government alike) haven't been taking the breach threat seriously enough to implement and routinely test their data security. Be it the result of carelessness or falling prey to the targeted attacks of hackers, many institutions have shown that they're still not ready to meet the threat head-on.

Landmark arrest

Albert Gonzalez is the computer genius-cum-master-hacker accused of helping perpetrate some of the biggest data breaches in U.S. history. According to federal indictments, Gonzalez helped orchestrate the attack on TJX, the company that owns TJ Maxx stores,

Gonzalez stands accused of pulling the two biggest hacking capers ever recorded. His scams and his arrest helped make identity theft headlines in 2009.

Monster.com

Indeed, Heartland and Hannaford Brothers weren't the only companies making headlines in January. The popular jobs site Monster.com also found itself in the news after its announcement that someone had illegally accessed a database containing Monster.com user IDs and passwords, names, e-mail addresses, birth dates, gender, ethnicity, and in some cases, users' states of residence. It wasn't the first time the popular jobs site ran into a data security snafu. The first occurred in August 2007, when intruders placed malware on corporate systems that was able to garner contact details for 1.3 million users.

After the most recent attack, Monster officials and outside observers were concerned that perpetrators would use their newly acquired contact information to perpetrate targeted phishing attacks — that is, that they would send out e-mails, under the guise of official Monster correspondence, intended to encourage users to download "tools" or "access agreements" supposedly needed to access accounts (nevertheless, when a cyber-criminal asks you to download something, chances are it's usually a malicious file).

So far, we haven't heard anything about follow-up attacks related to the Monster intrusion, but it stands as an important reminder to remain savvy about handling unsolicited e-mails, especially ones that ask for personal or login information or invite you to download software.

Stealing from the top dog

It was reported in 2009 that identity thieves scored probably their biggest victim ever: Federal Reserve Chairman Ben Bernanke. A pickpocket ring calling itself "Cannon to the Wiz" stole the purse belonging to Bernanke's wife, Anna, from a coffee shop in Washington, D.C. in the

Gonzalez stands accused of pulling the two biggest hacking capers ever recorded. His scams and his arrest helped make 2009 a big year for identity theft. With him off the streets, hopefully we will have no more blockbuster breaches in 2010.

the average large-scale data security lapse costs a corporation millions of dollars to investigate, close the breach, and defend itself against class-action lawsuits, many companies may be keeping their breaches quiet.

Second, even if the number of breaches has actually declined, the number of personal records compromised has leapt from 35 million in 2008 to more than 220 million in 2009.

Of course, there was one particular reason for the jump: the Heartland Payment Systems and Hannaford Brothers breaches which, combined, accounted for the loss of 130 million credit and debit card numbers last year, thanks to Albert Gonzalez (whom we cover in our next entry).

stealing 94 million personal records. He also allegedly participated in attacks on Heartland Payment Systems and the Hannaford Brothers supermarket chain.

Gonzalez was charged with possession of fake credit cards in 2003 in a case involving more than 18 million stolen personal records. He escaped a jail sentence by helping the U.S. Secret Service convict 18 of his co-conspirators. But almost as soon as that case was over, Gonzalez went back to stealing identities. By the time federal agents finally arrested him in 2009, he was wanted on identity theft-related charges in three states. Gonzalez eventually pleaded guilty in federal courts up and down the Eastern Seaboard for plotting the hacking attacks on TJX, Office Max, Barnes & Noble, the Dave & Busters restaurant chain, and many other companies.

summer of 2008.

The purse contained credit cards and the couple's joint checkbook, which the crooks used to cash checks under Bernanke's name. Members of the crime crew have been charged in federal court with stealing more than \$2.1 million from hundreds of identity theft victims.

Given Bernanke's position as one of the most powerful individuals in the world economy, this would be akin to stealing a tank from Defense Secretary Robert Gates and using it to knock over convenience stores.

The lesson here for consumers: keep an eagle eye on your belongings. And if you do find yourself the victim of a purse- or wallet-snatching, notify your credit and banking institutions, scan your accounts daily for signs of fraud (reporting any suspicious transactions immediately), and monitor your credit reports.

Facebook scammers: When a friend isn't a friend

Some Facebook users received rather strange messages from their online "friends" in 2009— instant messages suggesting that the friends were stranded in London and needed money to get home. In fact, they were impostors who'd hijacked Facebook accounts to raid lists of friends, looking for people to scam. The bad guys obtained account information with an old-fashioned phishing scam, building a fake Facebook page and luring victims into "re-confirming" their login information.

Before 2009, many of the vulnerabilities of peer-to-peer and social networks remained largely hypothetical. This year, they came out into the open. As annoying and frightening as they may have been, perhaps they provide an

The Biggest Data Breaches of 2009

1. Heartland Payment Systems, 7-Eleven and Hannaford Brothers (a.k.a. Worst Breach Ever)

Total number of records stolen: 130 million

2. National Archives and Records Administration

Total number of records lost: 76 million

3. Check Free Corp.

Total number of records lost: 5 million

4. Health Net

Total number of records lost: 1.5 million

5. Oklahoma Department of Human Services

Total number of records lost: 1 million

6. Arkansas Department of Information Systems/ Information Vaulting Services

Number of records lost: 807,700

7. Network Solutions

Number of records: 573,000

8. Virginia Department of Health Professions

Number of records at risk: At least 531,400, possibly over 8 million

9. phpBB.com

Number of records stolen: 400,000

10. University of North Carolina at Chapel Hill

Number of records stolen: 236,000

opportunity for consumers, military contractors and government agencies to finally learn to better manage their files and personal data online.

Even the savvier of Web users have fallen for these scams, which should make all of us consider being more conservative in conducting our online lives. Unfortunately, 2009 was the year of "TMI (too much information) is not enough" — and there are few signs yet of a turnaround.

Failure in the clouds

Peer-to-peer and social networking programs are a boon to efficiency and connectivity. In 2009, we learned they also present a big threat to our identities.

Within weeks of Barack Obama's inauguration, secrets about his official helicopter were discovered on an Iranian computer. Marine One, the heavy-duty chopper that transports the president, was exposed by a government contractor in Bethesda, Md., which allowed its affiliates overseas to access sensitive files via a peer-to-peer file sharing program.

Someone based in Iran used the program to download detailed information on Marine One's engineering and communications systems, according to Tiversa, a Pennsylvania-based company that monitors activity in such networks.

"We're noticing it out of Pakistan, Yemen, Qatar and China," said Bob Boback, CEO of Tiversa. "They are actively searching for information disclosed in this fashion because it is a great source of intelligence."

It's not just foreign nationals who learned how to exploit P2P networks in 2009. Gregory Kopiloff, 35, was sentenced to 51 months in prison for stealing tax, banking and credit card information shared over file-sharing networks.

At federal agencies: where did all those computers go?

Not all the big identity theft problems of 2009 occurred in the nebulous world of cloud computing, however. General Accountability Office found that large federal agencies continue to do a poor

job performing the most basic function of data security: Preventing hardware from leaving the building.

Many federal agencies could not account for all the laptops, hard drives and other computer devices containing sensitive documents. Were those pieces of software safely shredded? Stolen by disgruntled employees? Lost in a desk drawer? Many federal agencies did not know.

In one case, the National Archive and Records Administration lost a hard drive containing a terabyte of data including the personally identifiable information of White House staff members and visitors during the Clinton administration.

“The Federal Trade Commission blew three chances in 2009 to begin enforcing the Red Flags Rule, regulation mandated by the Fair and Accurate Credit Transactions Act of 2003 requiring creditors to watch for warning signs of identity theft.”

The GAO also found that NASA failed to properly encrypt sensitive data or secure computer hardware; the Los Alamos National Laboratories failed to monitor users or securely defend its network of 3,900 classified computers; and the IRS did not encrypt sensitive taxpayer data or create adequate access controls for its computer systems.

“As a result,” the government investigators wrote about the IRS failures, “sensitive information used by the federal government, financial institutions, and law enforcement agencies to combat money laundering and terrorist financing is at an increased risk of unauthorized use, modification, or disclosure.” None of these risks were new in 2009. The GAO has found similar vulnerabilities

going back to the mid-1990s. But they were big gaffes, involving the government institutions that manage our economy, our space flights, our taxes and our nukes. Given the size of government bureaucracies and the complexity of their computer networks, this problem threatens to grow even larger in 2010.

The FTC’s flake-out

2009 was the year of the Big Flake-Out when it comes to government protecting citizens from identity theft. The Federal Trade Commission blew three chances in 2009 to begin enforcing the Red Flags Rule, regulation mandated by the Fair and Accurate Credit Transactions Act

of 2003 requiring creditors to watch for warning signs of identity theft, and plan how to react if they suspect identity theft in a credit application.

Financial institutions like banks and credit unions began complying with the Red Flags Rule in 2008. But lawyers, doctors and retailers spent 2009 lobbying against the rule, saying it had been “sprung” (even though red flags have been debated for more than a decade). The lobbyists prevailed, however, pushing FTC to postpone enforcement for a fourth time.

Now the Red Flags Rule won’t take effect until June 2010 (unless the lobbyists succeed in getting yet another extension). Hopefully, consumers can put enough pressure on Congress and the

FTC to take this big step forward against identity theft.

Regulators flex HITECH muscles

For years after it passed Congress, the Health Insurance Portability and Accountability Act (HIPAA) was a paper tiger. It contained tough new regulations requiring health care companies to protect patient privacy. But no government agency had the power to actually enforce it.

That changed in 2009 when Congress passed the HITECH Act, giving state attorneys general the power to sue companies for violating patient privacy. Right away, two states flexed their new muscles. In Connecticut, Attorney General Richard Blumenthal went after two companies, Health Net and Anthem Blue Cross Blue Shield, for losing consumers’ private health data and failing to notify anyone of the breaches.

Health Net lost an external hard drive containing 1.5 million sensitive records. It failed to notify consumers about the breach for six months, well past the two-month deadline required by HITECH, an “inexplicable and inexcusable delay,” Blumenthal said. Both Blumenthal and Arizona Attorney General Terry Goddard are investigating the lapse.

At Anthem Blue Cross Blue Shield, a laptop stolen on Aug. 25 containing the names, addresses, Social Security numbers and other information exposed about 19,000 health care providers to identity theft. The theft was not reported for almost three months. Blumenthal said he would demand identity theft insurance and reimbursement for credit freezes for the victims.

Not long ago, Blumenthal would have been powerless in situations like this. Now, Blumenthal said, “I will vigorously and aggressively seek damages, penalties and other appropriate remedies.”

Opportunity on the horizon

Data brokers collect mountains of private information about American citizens with little oversight regarding how that information is gathered, verified or maintained. A bill passed in December by Congress may begin to change that. The Data Accountability and Trust Act would:

- Require brokers to verify whether the information they gather on individuals is accurate
- Allow consumers to correct incorrect information
- Require data brokers to notify consumers of data breaches, like the one in 2005 in which ChoicePoint inadvertently sold the identities of 163,000 people to identity thieves.

The bill passed the House on Dec. 8, and now moves to the Senate for consideration.

2009 was another opportunity-filled year for identity thieves. It also was another year of challenges for people who work to fight identity theft. Legislators and regulators passed some of the tests thrown their way, and failed others. The good news is that 2010 offers many opportunities for consumers, political leaders and bureaucrats to capitalize on the successes of 2009, and fix the failures. ■

He who every morning *plans* the transaction of the *day* and follows out that plan, carries a thread that will guide him through the maze of the most busy life. But where no plan is laid, where the disposal of time is surrendered merely to the chance of incidence, chaos will soon reign.

– Victor Hugo



2010

The Year of Accountability

Editorial by Adam Levin

Let's reflect for a moment on the year in identity theft. Is government taking steps to address the crime? Finally yes, but decidedly not fast enough. Is law enforcement trying hard to attack the source? Yes, but it is still woefully underfunded, undertrained and ultimately outgunned as it confronts an ever-evolving, highly sophisticated enemy of nearly unlimited resources. So who ultimately bears the responsibility for making sure a problem affecting millions of people doesn't become a personal one?

You. ◀

Frankly, it's outrageous that hundreds, if not thousands, of organizations have left consumer data as ripe for the picking as a lawn ornament on a college campus. And it's certainly not a consumer's fault that quick and easy credit has, for many, made for quick and convenient crime. But this is the hand we've all been dealt. Now it's time to play the cards. The challenge: maintaining privacy in an increasingly public world.

You limit the number of credit and debit cards you carry. You never leave your license in your glove compartment or your laptop in your trunk. You guard your mail. You safeguard your most sensitive documents. You shred everything. You're careful about your online activities and keep all of your anti-virus software up to date. You constantly try to limit the amount of personal information traveling from your possession into the great unknown: to wit — you don't provide personal data to folks who call you, don't open suspicious attachments or click on links that appear in e-mail and you don't expose your innermost secrets on social networking sites. Sadly, this is still not enough. To paraphrase the oft-repeated sports adage: You can't stop identity theft, but you can work hard to contain it. Now what? You can start with your credit report.

Start **with** yourself

Thanks to a federal law passed in 2003, consumers have had the ability to obtain a free credit report once a year from each of the major credit reporting agencies: Equifax, TransUnion and Experian. Certain states mandate even greater access. Everyone should do this at least as often as the law permits. If somebody has committed new account fraud against you — that is, they've set up unauthorized accounts — you'll more likely be able to spot it in your credit file, and address the situation right away. By

detecting and reporting the crime, you're not only saving yourself from potential ruin, you're potentially stopping a criminal from exploiting others.

Another major reason to check your credit regularly should be obvious — you should want to know what's going on with it, especially in this economy. Nevertheless, consumers aren't exactly flocking to pull their reports. This disappointing news comes from a recent

“If you've been offered free credit or fraud monitoring (very often, in response to the breach of a database containing sensitive personal identifying information), don't look a gift horse in the mouth. These are highly useful tools that can make the job of managing your identity so much easier.”

survey from Credit.com that found that some 46 percent of consumers had either never seen their credit reports or hadn't checked them in the past 12 months.

Beyond routine checking of credit reports, other habits can make you a more responsible consumer. Carefully inspect your credit card bills, bank statements, and every other utility or bill you pay every month. To be even more proactive (and why shouldn't you be?), spend just five to ten minutes a day reviewing transactions in your bank accounts and credit card accounts. If you see anything that looks suspicious — a purchase you didn't make at a store you've never visited, for example — investigate. If you find that someone has posed as you to make that purchase, immediately contact your financial institution or credit card company, call

the fraud department of any of the three credit reporting agencies, report the identity theft to your local police, your state attorney general and the Federal Trade Commission.

Some situations pose a greater risk than others. If you've been offered free credit or fraud monitoring (very often, in response to the breach of a database containing sensitive personal identifying information), don't look a gift horse in

the mouth. These are highly useful tools that can make the job of managing your identity so much easier. It all boils down to accountability. Remember, no one has a stake in protecting your financial security greater than yours. No one has more intimate knowledge of your transactions than you.

Being accountable to yourself as a consumer can be difficult, but in the long run it's imperative to your well-being.

While we're on the topic of accountability...

The **private** sector and the **bottom** line

Most data breaches start with organizations failing to hold themselves accountable for the huge databases of

information they gather about every aspect of our lives. Indeed, for decades, most businesses have fiercely protected their trade secrets and intellectual property, and since 9/11 many have focused on physical security measures. But when it comes to securing an equally precious asset — the personal identifying information of their customers or employees — they drop the ball.

Like years past, every week in 2009 brought news, “Groundhog Day”- style, of another data breach at another organization that put people in danger of identity theft. Sure, sometimes breaches are the work of sophisticated

“Like years past, every week in 2009 brought news, “Groundhog Day”- style, of another data breach at another organization that put people in danger of identity theft. ”

hackers. Others, very often, are the result of a preventable mistake — an accidental e-mailing of sensitive data, use of corporate computers for private social networking, employees losing discs, back-up tapes falling off the back of trucks, or the loss or theft of a laptop containing very sensitive, and completely unencrypted, data.

In 2010, this must change. Why? If the potential damage to consumers’ lives doesn’t convince business leaders of this, here’s another compelling angle: With all the costly regulatory actions, lawsuits and publicity that followed giant data breaches like TJX and Heartland this year — both the result of cyber-intrusions — businesses are learning the hard way

how much it costs to ignore data security issues. Thus far, Heartland reports that its breach-related expenses have reached in excess of \$30 million (most recently, it paid out \$3.6 million to settle claims with American Express); TJX reported that the cost of its 2006 breach has reached \$117 million and potentially is still climbing. That’s just the calculable cost. But what about the incalculable cost of disintegration of partner relationships and erosion in consumer confidence?

Certain aspects of data security are — plain and simple — not so plain and simple. Information technology professionals charged with securing corporate networks and databases from

outside intrusion, for example, have a mandate that requires a constantly evolving technical expertise. Other data safeguarding concepts — like limiting sensitive data access only to those who require its use, controlling what gets circulated externally and encrypting personal information — are easier to grasp and implement at an institutional level. Security protocols should be uniform across an entire company and computer systems should be monitored routinely for suspicious activity.

Companies must also have plans in place for how to react when there is a data loss. That will reduce the potential fallout of identity-related fraud, and help them comply with the Red Flags Rule, which, if

the FTC allows, will take effect for a large body of credit-issuers in June 2010.

In light of the current economic situation, companies simply can’t afford to overlook the possibility of insider identity theft. Unfortunately, circumstances have made the leakage of data to the outside all the more emotionally and financially lucrative. Again, limiting employee access to sensitive info could help, as well as conducting criminal background checks on individuals who will be in privileged positions.

These guidelines aren’t red tape, they’re good common sense. If you argue that establishing meaningful security protocol and preventive measures impairs the bottom line, ask management at Heartland and TJX — if they could do it all over again, would they rather have paid a lot less a couple of years ago, or the whole lot more they’re paying now?

Government: The most complicated player of all

Government at all levels has the power to help curb or unintentionally exacerbate the identity theft problem in 2010. Whether they use this power for good, or negligently or incompetently abuse it, remains to be seen. Government must lead by example by taking its own data protection practices seriously. Given the vast amount of private data the federal government maintains on citizens, a repeat of major breaches like the one in 2006 at the Department of Veterans Affairs, which exposed 28.6 million veterans to identity theft, could be devastating.

Enter the much-anticipated “Cyber Czar.” Just before Christmas, President Obama named former Microsoft and eBay executive Howard A. Schmidt as permanent chief of the nation’s cyber-

security front. Mr. Schmidt has serious government and industry cred, but his new post already looks to be hamstrung by economic considerations. He'll be answering to both the National Security Council and the National Economic Council; serving two masters in the interest of developing cyber-policies that won't be detrimental to the economy. Of course it's important to develop smart policies that are economically feasible, but there's obvious potential here to undermine the integrity of good, solid cyber-security infrastructure in the name of saving money. In fact, it's already in the works.

Unless the new Cyber-Czar stops it, other federal agencies are moving forward with economically friendly plans that could well compromise our identities. Vivek Kundra, Chief Information Technology Officer of the United States, said in a recent speech that he plans to increase the government's use of cloud computing services.

Such a move is premature and dangerous. Cloud networks, as they currently operate, have no legal obligation to keep data secure or private. As Kundra pushes government agencies to adopt the cost-saving cloud networks, many officials are concerned that the networks lack critical security standards.

On the other hand, the passage in December 2009 of the Data Accountability and Trust Act was great news. This legislation is intended to reign in the Wild West-style business practices of the data broker industry, establishing minimum standards of

fairness and accountability to protect consumers. The act requires that brokers verify whether the information they gather on individuals is accurate, allow consumers to correct incorrect information, and requires data brokers to notify consumers of data breaches. This is among the best legislation from Washington in the fight to protect consumers' identities in years. However, it is premature to uncork the champagne. In 2010, the Senate must pass it, and President Obama must sign it.

Here's a big test for the federal government in 2010: what will come first, universal peace, or enforcement of the Red Flags Rule, which requires creditors to watch for warning signs of identity theft, and plan a response for when they detect a case of suspected identity theft? Bowing to pressure from lobbyists and members of Congress, the FTC has postponed implementation of the rule four times. The new deadline is June 1, 2010.

The new deadline must be do-or-die. The FTC must hold creditors accountable to the law, which it passed almost seven (that's right, seven) years ago. And it's crucial that Congress, rather than inhibit the FTC, sees the light and supports the agency's efforts to help contain identity theft.

At the state level, attorneys general in big states like Texas, Ohio and New York should follow Connecticut's example and use their power under the HITECH Act to hold medical companies accountable for data breaches. Generalized warnings about data breaches and identity theft

can fade into the white noise of the 24-hour news cycle. By suing companies that expose consumers to fraud, attorneys general have the opportunity to hold people accountable for their actions and raise the profile of this important issue.

As we emerge from an unprecedented global financial meltdown born of unbridled lending, borrowing and spending, hopefully we have begun to understand that such irresponsibility comes at a very steep price. So, too, does the cavalier treatment of our identities by government, business and, indeed, by so many of us. Time and again, that cost is borne out on individuals — often profoundly so, as they're forced to squander time and money clearing up fraudulently damaged credit and wounded reputations. It's borne out on retailers who must find a way to cover costs of merchandise stolen with fraudulently obtained store credit, and it's borne out on financial institutions that take a hit when bogus accounts are opened at their institutions. Further, it can endanger our health, subject us to potentially groundless arrest, aid terrorism and compromise our national security.

It's abundantly clear that we all have a stake in this issue. So why does everyone continue to make the same mistakes yet expect change to arrive as if by magical conveyance? Here's a notion: let's make 2010 a year of accountability — corporate accountability, government accountability, and of course, personal accountability. ■