

Stay Grounded in the Cloud

Storm of Cloud-Computing Services Looms on Horizon

Many people have their heads in the cloud—cloud-based services, that is—and they don't even know it.

Consumers access and share information using remote server networks whenever they log on to Facebook, edit photos on Flickr, blog with WordPress, or create files on Google Docs.

Companies rent backup data storage from providers such as Amazon.com or buy computing power from a vendor instead of using an in-house server—at a huge cost savings. Some firms use Web-delivered software programs such as Salesforce.com, which helps salespeople keep track of customer information.

[Continued on page 3](#) ▶

Outlook: Cloudy with Little Chance of Privacy

Popular Technology Puts Security in Peril

Consumers needn't look far for examples of cloud-based services gone wrong. Still, they're often surprised when they lose documents, photos and other data stored online.

Consider these stories: Photographer Morgan Tepsic lost more than 3,000 photos on Flickr after a hacker deleted them from his account. A Community Newspaper Holdings employee inadvertently sent sensitive company information through Google Docs to a New York Times reporter instead of a co-worker. And Google accidentally shared thousands of private Google Docs files with unauthorized users due to a computer glitch. [Continued on page 4](#) ▶



In the past few years, businesses have undergone a significant shift in the way they share and manage valuable data. They've moved away from confining proprietary information to their own networks. Now, they entrust third parties to handle once closely guarded data. The factors behind this pendulum swing aren't surprising: convenience and affordability. Businesses of all sizes save money on software, hardware and technical support—but not without a measure of risk.

In this month's newsletter, we explore cloud computing, a topic that's been generating a lot of debate in the computer industry. We give an overview of what it is and why it's more than a passing trend. Plus, we share expert tips that businesses and consumers should consider before making the leap to the cloud, that is, storing their information on servers outside of their direct control.

We also introduce a new, ruthless class of identity thief: community predators who take advantage of people of a certain age, income level or ethnicity. This issue's case study reveals how our Fraud Resolution Center helped a couple solve the mystery behind their missing \$40,000 refinancing check and \$24,000 worth of bills for items they never bought, including a custom, four-wheel ATV.

Finally, be sure to check out our "Hits & Misses," a roundup of the latest fraud-related news, as well as a guest Q&A with the nationally recognized mortgage and real estate fraud expert Rachel Dollar.

As always, we hope you will enjoy.

Matt Cullina
Chief Executive Officer,
Identity Theft 911

In this issue...



Departments

- 5 **Case Study:** Learn how to spot community predators who prey on people of a certain age, income level or ethnicity.
- 6 **Hits & Misses:** A roundup of who's getting it right and wrong in the fight against identity theft.
- 7 **Ask the Expert:** Mortgage expert Rachel Dollar talks about new fraud trends triggered by the housing market crash.

These are examples of cloud computing, which, simply defined, is how we store and share data, applications and computing power on the Internet. In recent years, it's gone from an IT buzzword to the preferred way we use our computers because of its convenience and affordability. Users can instantly access and manage data from any location. Businesses of all sizes save money on software, hardware and technical support. However, experts caution that entrusting valuable data to a third party carries certain risks. Confidential information can be lost, stolen or delivered too slowly.

"If you entrust your data to others, they can let you down or outright betray you," said Jonathan Zittrain, a Harvard law professor and co-director of the [Berkman Center for Internet and Society](#). "Data stored online has less privacy protection, both in practice and under the law."

Cloud Generation

By 2020, most people will do their work "on the cloud"—online—instead of using software on their computers, according to a new survey from the Pew Research Center's Internet & American Life Project and Elon University's Imagining the Internet Center.

"Data stored online has less privacy protection, both in practice and under the law."

— Jonathan Zittrain, co-director of the Berkman Center for Internet and Society

The study acknowledged that many people already are using Internet-based applications for most of their tasks. Pocket devices have accelerated the shift to cloud computing because they lack storage capacity for large files like photos and music. People now elect to save these files remotely for easy access.

A new generation of future young professionals is growing up familiar with the convenience of the cloud. They depend upon it to stay connected via their iPhones and Android phones. So do their universities. Microsoft and Google have deployed cloud-computing services at universities worldwide. Microsoft reaches more than 11 million people in

10,000 schools in 130 countries. Google Apps for Education's website says 8 million students use its communication and collaborative tools for schools and universities.

Meanwhile, large cloud providers like Amazon, Microsoft, Google and AT&T are working to convince companies and government agencies to use their computer capacity instead of building in-house data centers. Many are jumping

people were concerned about the way cloud-based services actually operate. Nearly 90 percent of computer users said they would be "somewhat concerned" if they learned that online data storage companies sold their files to other people. And 80 percent of respondents would be concerned if companies used their private information in marketing campaigns.

Many big corporations and agencies are cautious about placing their operations

Cloud Components

The Cloud: Often used as a metaphor for the Internet.

Cloud Computing: How we store and share data, applications and computing power on the Internet.

Types of Cloud Services: Sites for data storage, video, tax preparation, health records, photography, social networking, and many more.

Source: Pew Study, World Privacy Forum

on board. NASA's Jet Propulsion Lab runs experiments on computers at Amazon, Microsoft and Google. This year, Netflix is moving its Web services—including customer movie queues and search tools—to Amazon-operated servers.

on another company's computers. They have reason to be. Intuit recently experienced an outage that left 300,000 of its business customers unable to access critical data—including employee payrolls and databases—for two days.

Users of cloud-based services should follow basic guidelines before handing over their sensitive information and business to cloud providers. PC Magazine analyst Samara Lynn offers these tips:

- Keep critical data local. Decide which information stays in-house. Consider regulatory compliance issues.
- Nail down a provider's disaster recovery and contingency plan before signing a contract.
- Develop a plan that combines cloud and local infrastructure to store and process data.
- Consider using a hot site, a fully functional facility, where customers can access services in the event of a disaster.

Outages like Intuit's won't slow the move to the cloud, Lynn writes in her regular column. But they remind customers to stay on guard and prepare for the worst. •

To be sure, some industry players say the excitement over cloud computing is all hype. Marketing of the cloud has overshadowed real innovation, they say. Oracle CEO Larry Ellison called it another example of the trendy nature of the computer industry, which he likened to women's fashion.

Outlook: Hazy

The main challenges people and businesses interfacing with cloud-based services face are: privacy, security and compliance issues, the Pew study reported.

A separate Pew poll found that most

These worst-case scenarios highlight some of the pitfalls of working in the cloud. Despite the benefits of sharing and storing information online, privacy experts say it puts user information at risk. Not only is the data vulnerable to hackers, it is subject to the policies and practices of the cloud provider.

“The identity theft problem continues to escalate, in part, because it’s too easy for companies to collect personal information and too difficult for individuals to safeguard it once it’s in someone else’s possession,” said Marc Rotenberg, executive director of the Electronic Privacy Information Center.

A Few Drawbacks

Experts point out that cloud companies’ privacy policies may give users a false sense of security. The reality is they often provide scant protections.

For example, most companies’ privacy policies only cover personally identifiable

“The identity theft problem continues to escalate, in part, because it’s too easy for companies to collect personal information and too difficult for individuals to safeguard it once it’s in someone else’s possession.” — Marc Rotenberg, executive director of the Electronic Privacy Information Center

information (PII), defined as a person’s name, Social Security number, birth date, and mother’s maiden name. But there’s a lot of other data that can identify users—bank account numbers or home addresses—that falls outside this narrow definition. And it’s not protected by most policies.

Another catch: Cloud-services providers like Google Docs and Symantec, a leading maker of computer security software, voluntarily comply with all subpoena requests for documents. That means anyone, say a business competitor or ex-spouse, could gain access to a user’s private documents without his knowing about it or having the opportunity to

challenge it. Had the information been saved on the user’s private computer, he would have the right to fight the subpoena, search warrant or court order.

Cloud providers often retain the right to view user account information, as well as the documents a user clicks on or displays on his computer monitor, including everything that is saved to the company’s servers. They also retain the right to share this information with the other divisions and third parties, including advertisers. They may use the information to identify a user’s geographic location. And many retain the right to copy, use, and publish user documents whenever they choose, or to share that data with others, according to a [World Privacy Forum report](#).

Some cloud providers can change their privacy policies at any time. And in some cases, they also have the right to deny users access to files if they stop paying monthly bills or violate rules.

Laws Have No Teeth

Privacy laws are almost as weak as corporate privacy policies, experts say.

The Patriot Act empowers the Federal Bureau of Investigation to access users’ online activities from service providers without informing users. A loophole in the Fair Credit Reporting Act says that once a third party retrieves users’ private information, such as a credit report, it no longer counts as private.

The Stored Communications Act was designed to protect electronic communications like email and online documents. But a loophole allows anyone

to legally access private documents as long as the provider grants access. The documents can be retrieved without the author’s permission.

“This means that even if the author has not authorized anyone to access his or her private documents, a lot of people could still be looking at them, copying

Tips for Consumers

- Read the Terms of Service before placing any information in the cloud.
- Don’t put anything in the cloud you would not want the government or a private litigant to see.
- Pay close attention to whether the cloud provider reserves the right to use, disclose, or make public your information.
- Read the privacy policy before placing your information in the cloud.
- When you remove your data from the cloud provider, does the cloud provider still retain rights to your information? If so, consider whether that makes a difference to you.
- Will the cloud provider give advance notice of any change of terms in the terms of service or privacy policy?

Source: World Privacy Forum

them and doing whatever they want with them,” says David Johnson, a Los Angeles attorney who specializes in commercial and digital media law. •

Broken Trust: Community Predators Target Vulnerable Consumers

In 2008, Christina and Francisco, a middle-aged couple with four children, sought to lower their monthly mortgage payments and get some extra cash by refinancing their home.

They were referred to a mortgage broker who was popular in their close-knit Hispanic community in California. Like them, the broker was bilingual. He worked hard to earn the couple's trust: He met them at their home and got to know their children. He assured them their paperwork would go through, allowing them to replace their old loan with one that was extended over a longer time period. They could take out the difference—\$40,000—in cash.

Their paperwork went through, but the couple never saw the money. Creditors began demanding payment for goods Christina and Francisco never bought. In a matter of months, their trusted broker had stolen their identities to open credit cards, cell phone accounts and buy extravagant items including a Polaris custom four-wheel ATV and high-end lawn equipment at John Deere. The couple were \$24,000 in debt.

The perpetrator is part of a ruthless class of identity thief who takes advantage

Mark Fullbright, an Identity Theft 911 fraud specialist. "This allows them to steal and commit identity fraud without hindrance."

Christina and Francisco's homeowners insurance put them in touch with Fullbright at Identity Theft 911. It didn't take long for him to determine who the culprit was. Fullbright immediately put the couple's credit files under a 90-day fraud alert, which asks creditors to verify information with individuals before extending credit. He encouraged

to mention their sense of trust—took a temporary hit.

When Christina and Francisco confronted the broker, he was savvy enough to claim that he, too, was a victim of credit card fraud. He even accompanied Christina to the police station, filed a fictitious report and kept an eye on what she wrote in her own report to see if it mentioned him. Then he skipped town.

"I just don't trust anyone anymore," she said.

Consumers who suspect wrongdoing should take immediate action, Fullbright said. File reports or complaints with these institutions: a local police station, a state attorney general's office, the Better Business Bureau and the Federal Trade Commission.

The couple no longer receive calls from creditors. But they continue to monitor their credit files and hope the culprit is arrested so no other families go through the same, devastating experience.

"Without Mark we wouldn't know what recourse was available and what steps to take," Christina said. "He really showed us what to do."

"Community predators count on their victims to trust them completely. This allows them to steal and commit IDT fraud without hindrance."

— Mark Fullbright, Identity Theft 911 fraud specialist

of people of a certain age, income level or ethnicity. Identity Theft 911 calls these types of criminals "community predators." They count on their victims' vulnerabilities—language and cultural barriers or inexperience—gain their trust and strike when the victims least expect it, experts say.

"Community predators count on their victims to trust them completely," says

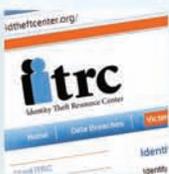
the couple to file a police report, which allowed them to extend their fraud alert services to seven years. And he worked with multiple collection agencies to explain they were trying to collect from the wrong people.

The couple weren't held responsible for the debt, all of which was removed from their accounts and credit reports with Fullbright's help. But their credit—not

Hits



The number of pending cybersecurity measures on Capitol Hill—40 total—means Congress may be getting serious about protecting the nation's government and private networks. Democratic Sens. Joe Lieberman, Tom Carper and Republican Sen. Susan Collins have co-authored a bill receiving a great deal of attention. It would grant the president emergency powers over the Internet; establish a White House Office of Cyberspace Policy; and reform the Federal Information Security Management Act, an eight-year-old law that governs how federal agencies secure IT systems. Lieberman is confident the bill will pass the Senate before year's end. He anticipates combining it with other legislation under consideration by Congress.



The Identity Theft Resource Center sees a silver lining in its study on the aftermath of identity fraud: Victims are spending less time and money on resolution efforts. The study found that in 2009 victims spent an average of \$527 dealing with accounts taken over by attackers. That compares with \$741 a year earlier. Meanwhile, victims in 2009 spent an average 68 hours repairing damages from compromised accounts. That's down from 76 hours the previous year. The San Diego-based center provides consumer support and education about identity theft and data breaches.

Misses



A former Los Angeles County social services worker allegedly preyed upon the very people he was supposed to help when he stole their identities to commit tax fraud. Trang Van Dinh of Glendale, Calif., filed bogus tax returns using his indigent clients' identities to obtain \$1 million in tax refunds, authorities say. An indictment against the 62-year-old claims he sought \$2 million in refunds using names, Social Security numbers and other personal information of the 176 people he handled in his caseload.



When a new gadget takes the tech world by storm, any security glitch is bound to attract intense scrutiny. Apple found itself on the hot seat last month when a hacker group accessed iPad user email addresses by exploiting a security hole on AT&T's website. The list of 114,000 users included military personnel, media elite and high-ranking politicians ranging from New York City Mayor Michael Bloomberg to White House Chief of Staff Rahm Emanuel. AT&T says it fixed the problem. The Federal Bureau of Investigation has launched an investigation.



Q&A: Rachel Dollar

Mortgage and Real Estate Fraud Expert

When it comes to who's scamming whom in the real estate world, Rachel Dollar has their number. Dollar, a nationally recognized mortgage and real estate fraud expert, edits the popular [Mortgage Fraud Blog](#), which tracks stories on the topic nationwide. She says the housing crash triggered the arrival of new kinds of fraud. Dollar took time from work at her Santa Rosa, Calif.-based law firm Smith Dollar, PC, to discuss loan modification schemes and other fraud trends.

What are the latest scams in the mortgage and real estate world?

Mortgage modification scams are a growth area. There are desperate borrowers out there who will pay a company a few thousand dollars to negotiate a modification with their lender. But often, the company doesn't even contact the lender. Or it tells the borrower to "stop paying your mortgage so you can pay us." Then it pockets the money and never obtains a modification.

Short sale fraud is also a big one, where there is a misrepresentation of a borrower's ability to continue to pay, or of the value of the property, or the purpose of sale. They'll negotiate a sale of, say, \$200,000 on a property in which the homeowner owes the bank \$250,000. They then contact the lender and talk the lender into taking a short payoff of only \$180,000. The short sale from the lender often closes concurrently with the higher priced "flip" to the new buyer.

The transaction can take place in a couple of seconds since the money is held in concurrent escrow accounts. The new buyer's loan is used to fund the short sale to the middleman. The middleman effectively sells the property before he owns it and keeps the profit.

What kinds of fraud occurred during the boom years?

Mostly it was fraud for housing—people inflating their reported income to get houses, either to live in them or have as an investment. There were a lot of Stated Income loans, where you could easily lie about your income (to buy more house than you could afford with the intent to flip it). Those loans are no longer available. The regulators have required the lending institutions to underwrite with an eye to the borrower's actual ability to pay. People can no longer get 80-20 piggyback loans, in which a property is purchased using more than one mortgage from two or more lenders and requires no down payment.

Any evergreen scams?

Investment clubs. Ringleaders approach people to invest in property. They say, "We'll do everything: choose it, renovate it, find renters, and you'll cash out at closing." But they don't do anything and keep the money. Often at those "Make Money in Real Estate" seminars, ringleaders will target people afterward and try to get them to join their club. There was one woman who wanted to buy three condos but ended up owning 98!

What is the profile of today's mortgage fraud perpetrator?

According to the Federal Bureau of Investigation, 80 percent of the frauds involve industry insiders, who know how to manipulate the system. The mortgage modification scammers are generally attorneys or former subprime mortgage brokers. With short sale scams, a lot of times it's real estate agents.

Who are the victims?

The lenders; they don't get their money back. But sometimes homeowners and home buyers are also victimized. Generally, the borrowers and straw buyers lose their credit. A straw buyer knowingly obtains a home loan for someone who can't buy it themselves.

Is this level of fraud a sign of the times?

There has always been a degree of fraud. It's not quantified, but I think it has increased the last decade. On the fraud prevention side, it's impossible to keep up with. Although law enforcement is aggressive in pursuing the cases, there's a huge volume. And we'll go through the whole thing again because real estate is cyclical. Since the mid-1800s the housing market has boomed every 18.3 years. •