

How to Build Privacy Into Customer Authentication

By Jay Cline

April 22, 2004 12:00 PM ET

Reports of worsening identity theft are pressuring companies to adopt stronger methods of making sure they know the identity of their customers. Most customers will find this additional layer of security comforting. But the more invasive authentication methods—biometrics, especially—have people worried that they'll lose their privacy in the process. How can businesses authenticate their customers without scaring them away? By putting the consumer in control throughout the authentication process.

Since 9/11, companies have been re-examining how they confirm that their customers are who they say they are before giving them access to systems and accounts. The 9/11 hijackers showed how easy it was for deadly criminals to pass through society making important transactions using unchecked credentials.

The next time you call your Internet service provider, for example, you'll probably have to pass through two or three filters before you can change your service. The ISP will check its caller ID to verify your phone number and then ask you to verify your name and address, and it may ask for one more piece of information.

For this third piece of information, an emerging trend has been to ask you for the answer to a "secret question" you set up when you open an account, such as a PIN, the name of your pet, your birthplace or your mother's maiden name.

For customers like me who are privacy sticklers, this is a welcome

improvement. I'm more certain that an imposter would be lacking all the right pieces of information to break into my account.

If you're not comforted by this trend, you should try the experiment I did last month. I accessed my top 25 accounts and noted what information the companies required from me to gain access. I found that in half of the cases, my favorite businesses required three or more pieces of personal information ([see Table 1](#)). This was rarely the case a few years ago.

But not everyone is excited about this development. Giving companies more information is dangerous, privacy advocates say, because no business has perfect security. And all customers have a point at which they'll abandon a registration process if too much information is required. Businesses may already be reaching that tipping point with their heightened authentication.

So how do companies strike the right balance? How can they simultaneously provide the levels of privacy *and* security that customers want?

There are two ways. First, companies need to adopt a tiered authentication policy. By tiered, I mean that the level of authentication should be directly related to the sensitivity of the account being accessed. The higher the sensitivity, the more credentials should be required ([see Table 2](#)). Customers will expect more scrutiny for financial accounts but will reject it for retail accounts.

Second, companies need to build privacy controls into their authentication process. The Center for Democracy and Technology has outlined a good set of requirements for what businesses should consider to reassure customers that they're in control of the authentication process ([see Table](#)

3). Customers want to know what's being collected about them, how it's being collected, how it's being used—and how they can confirm all of that.

Those two building blocks make up a robust authentication strategy. And a strategy like that is what your company needs before it even thinks about jumping into biometrics. Otherwise you can count on scaring your customers back to where they came from.

Table 1: Financial Services, ISPs Toughest on Authentication

Some companies have added a third layer of remote-customer authentication. Below are the pieces of information that my favorite businesses required from me to check my account status over the phone.

Types of accounts	Caller ID or name and address	Account number	Social Security number, PIN or answer to a secret question
Credit cards, checking, 401(k), ISP	x	x	x
Student loan, department store credit, mortgage, car loan, car insurance, retail loyalty program	x	x	

Utilities, book club	x		
----------------------	---	--	--

Table 2: Adopt a Tiered Authentication Policy

Companies should vary how they authenticate customers by what type of account the customers are trying to access. Otherwise they risk scaring customers away.

Authentication levels		1	2	3	4
Risk of harm if identity falsified		Minimal	Low	Significant	High
Types of customer accounts in these risk categories		Online e-mail and newsletters	Non-degree learning, retail, utilities	Travel itineraries, ISPs, property insurance	Banking, debt, health and life insurance, tax, diplomas
Recommended credentials to require from customers to establish an account	E-mail address	x	x	x	x
	Name, address		x	x	x
	Phone number			x	x
	Date and place of birth			x	x

	Driver's license number				X
Recommended credentials to require from customers for ongoing account access	Password or PIN	X	X	X	X
	Account number		X	X	X
	Secret question			X	X

Table 3: Privacy Controls for Authentication

The Center for Democracy and Technology has developed a set of privacy principles that companies can implement to reassure customers who are concerned about authentication.

Privacy Principle	Definition
Provide notice	Individuals should be provided with a clear statement about the collection and use of information so they can make informed decisions.
Provide user control	Companies should obtain the informed consent of the individual before information is used for enrollment, authentication and any subsequent purpose.
Minimize collection and storage	Companies should collect only the information necessary to complete the intended authentication function.

Use individual authentication only when appropriate	Companies should design systems to authenticate individuals with their identities only when such information is needed to complete the transaction.
Provide accountability	Customers should be able to verify that companies are complying with applicable privacy practices.
Support a diversity of services	Individuals should have a choice of authentication tools and providers in the market -- privacy is at risk when individuals are forced to use one identifier for various purposes.