

# Calculating Today's Two-Factor Authentication ROI



PhoneFactor, Inc.  
7301 West 129th Street  
Overland Park, KS 66213  
1-877-No-Token / 1-877-668-6536  
[www.phonefactor.com](http://www.phonefactor.com)

# Calculating Today's Two-Factor Authentication ROI

The average security breach costs an organization \$6.3 million, plus countless employee hours, customer confidence, and hits to your brand reputation. Passwords are often the weakest and most exploited link in an organization's IT security infrastructure, so investing in two-factor authentication to secure user access is a smart budget choice.

But what's the best solution available? And how do you convince the rest of the team that it's more critical now than ever to invest in two-factor authentication? Whether you are the final decision maker or you need to present your recommendation up the chain of command, this whitepaper will arm you with the necessary tools to make the case for two-factor authentication in your organization.

## Contents

Building a Case for Two-Factor Authentication	3
Attacks Increase as Hacking Becomes an Organized Crime	3
Quantifying the True Impact of a Security Breach	3
Why Is Two-Factor Authentication So Important?	3
It's All About the Bottom Line	4
PhoneFactor Delivers Strong Security and a Strong ROI	6
Two Easy Steps for Users	7
Strong Two-Factor Security	7
Cost Effective	7
Conclusion	7

# Building a Case for Two-Factor Authentication

## Attacks Increase as Hacking Becomes an Organized Crime

Across the world, data is under attack. Malicious data capture is no longer a sport for hackers in their spare time. It is a crime with a legitimate business model. Organizations now employ programmers dedicated to producing these threats. Many of these are based in Eastern European countries, but not exclusively. Cybercrime is now an important revenue sector for global organized crime both in the US and abroad.

## Quantifying the True Impact of a Security Breach

While it's difficult to pinpoint the exact costs of a security breach for one particular company, research does exist to quantify the average costs. According to research from the Ponemon Institute, the average security breach costs \$6.75 million with the average cost of each compromised record totaling \$204 (2009 Annual Study: US Cost of a Data Breach, Ponemon Institute). The costs of a data breach have risen dramatically since 2005 when the cost per record was just \$138.

These costs include investigation and forensics, credit monitoring services, legal fees and fines, customer support costs, but the most rapidly growing cost categories relate to increased customer churn and reduced new customer acquisition. Lost business accounts for 69% of the total cost of a data breach. This figure has increased dramatically over the last three years as customers continue to raise the bar of expectations. Customers demand that businesses maintain the highest level of trust and privacy and have little tolerance for vendors who do not meet these expectations. This is particularly true in the healthcare and financial services industries where customer churn rates are between 5.5% and 6.5%, compared to 3.6% overall (2008 Annual Study: US Cost of a Data Breach, Ponemon Institute).

## Why Is Two-Factor Authentication So Important?

Passwords are a known weak link and continue to be exploited at alarming rates. From simple phishing schemes to sophisticated, targeted phishing attacks, gaining access to a user's password is an easy and prolific attack.

Regulatory agencies agree. The Federal Financial Institutions Examination Council, for example, requires strong authentication for high-risk transactions. The Payment Card Industry Data Security Standard explicitly requires two-factor authentication for remote access to networks where credit card data is stored and processed. The Health Insurance Portability and Accountability Act (HIPAA) and various other industry regulations are following suit with increasing rigorous requirements for strongly authenticating users.

So what is two-factor authentication? Two-factor authentication is any two of the following: something you know, like a password or PIN number; something you have that can't easily be copied, like a credit card or token; and/or something you are, like a fingerprint or some other form of biometric.

In order to qualify as two-factor authentication, two items must be combined from different categories, so a PIN plus a password doesn't count as two-factor, since both items are something you know.

Furthermore, the authentication is materially stronger when deployed across two different channels, that is, when it's out-of-band.

Out-of-band authentication is becoming the new standard for authentication because of the added security benefits. With out-of-band authentication, an attacker must compromise two networks to obtain access to a user's account. He'd have to collect the two factors of authentication across two unique channels.

## It's All About the Bottom Line

What it comes down to is your bottom line. Corporate risk is rising and cybercrime is getting more organized. There is an increased frequency and intensity of attacks that put your business at tremendous risk. Two-factor authentication is an absolute necessity. However, budgets are being cut, and every penny is being scrutinized. In order to get budget approval, you have to build a business case for two-factor authentication.

While the risks associated with a data breach and the role of two-factor authentication in protecting your organization are clear, quantifying the

return on your investment in two-factor authentication can be more difficult. The following model uses both the Total Cost of Ownership (TCO) for two-factor authentication and the average risk and costs associated with a data breach to determine the Return on Investment (ROI).

Figure 2 maps out the costs of two leading two-factor solutions - security tokens, like those offered by RSA, and phone authentication from PhoneFactor. The chart is based on 2500 users for a two-year deal and includes both hard costs (licensing, support, etc) from the vendor and soft costs that will be incurred by your organization to deploy and support the solution (implementation, user deployment, help desk costs, etc).

<b>Total Cost of Ownership (2 Years)</b>		<b>Tokens</b>	<b>PhoneFactor</b>
<b>Average Solution Costs</b>			
Software License		\$100,000	Included
2500 Tokens		\$75,000	NA
Replacement Tokens – 10% Per Year		\$15,000	NA
Annual - Per User or Per Auth		\$40,000	\$100,000
<b>TOTAL SOLUTION COSTS</b>		<b>\$230,000</b>	<b>\$100,000</b>
<b>Deployment and Support Costs (Internal)</b>			
Deployment to Users	\$15 per device	\$37,500	NA
Deployment of Replacement – 10% Per Year	\$15 per device	\$7,500	NA
End User Support Calls - % of User with One Support Call a Year x \$20	25% tokens, 5% Phone	\$25,000	\$5,000
<b>TOTAL INTERNAL COSTS</b>		<b>\$70,000</b>	<b>\$5,000</b>
<b>TOTAL COST OF OWNERSHIP</b>		<b>\$300,000</b>	<b>\$105,000</b>

**Figure 1: Total Cost of Ownership**

These systems vary significantly in the amount of implementation and deployment time they require, and these costs are often hard to calculate. How easily and how tightly the system integrates with your existing applications and management processes is going to have a big impact on the internal cost. For solutions that require you to provision and ship physical devices, like security tokens, you can expect material internal costs for the initial deployment.

The other big cost component is maintenance and support. For example, users lose tokens – up to 10 percent a year – and replacements have to be provisioned and shipped, and until that replacement arrives the user is either locked out of the system or forced to bypass that additional layer

of security. Ultimately, this leads to user frustration, loss of productivity, increased helpdesk costs, and possibly non-compliance.

Figure 2 explains the next step, which is calculating the Return On Investment (ROI). Here we compare the two year TCO to the adjusted risk of a single catastrophic security breach.

Total Return On Investment (2 Years)	Tokens	PhoneFactor
2 Year Total Cost of Ownership	\$300,000	\$105,000
Adjusted Risk of Single Catastrophic Security Breach	\$843,750	\$843,750
Return On Investment - Percent	181%	704%
Return On Investment - Dollar	\$543,750	\$738,750

**Figure 2: Return On Investment (2 Years)**

If you remember, a single catastrophic security breach averaged \$6.75 million. So the third row is 12.5% of that \$6.75 million figure, assuming that you have a one-in-four chance (25%) of having a breach in that two year period and that you can cut that risk in half by adding additional authentication ( $25\% / 2 = 12.5\%$ ). A 2009 PhoneFactor survey of IT professionals indicated that 25 percent had experienced a breach at their current company.

Based on this, there are two ROI numbers calculated – a percentage and a dollar figure. Using this model along with the data on security breaches and the state of security today, you should have the tools you need to present a strong case for two-factor authentication.

## PhoneFactor Delivers Strong Security and a Strong ROI

As demonstrated by this model, PhoneFactor proves to be a strong value compared to other types of two-factor authentication solutions. PhoneFactor combines the high degree of security that you need to protect your company from today's attacks, with a solution that's easy to set up, maintain, and use. PhoneFactor works with any phone – landline or mobile – anywhere in the US and abroad. There are no tokens for users to carry and track, no software downloads to mobile phones, and no hardware devices to manage or purchase. PhoneFactor provides out-of-band authentication and offers real-time fraud alert capabilities.

## Two Easy Steps for Users

So how does PhoneFactor work? Users simply log into their applications – such as a VPN, online banking, e-mail, etc. – just like they do today. They enter their user name and password into the login interface, and instantly they receive a phone call. They answer the call, and press # or enter a PIN into the phone keypad to authenticate. It's that simple.

## Strong Two-Factor Security

By combining out-of-band authentication with real-time fraud alerts, PhoneFactor offers the strongest level of security on the market today. The PhoneFactor platform relies on the telephone network for the second factor of authentication, which ensures protection against keystroke loggers and man-in-the-middle attacks. PhoneFactor can be used to verify specific high-risk transactions, so even if the user's authenticated session has been hijacked, their transactions are protected. Not only does PhoneFactor prevent unauthorized logins and transactions, it notifies you instantly if a user's credentials have been compromised and an attack is in progress. Tokens and other security devices are simply not capable of alerting you to an attack.

## Cost Effective

Because there are no devices to deploy or manage and no software or certificates for end users to install, PhoneFactor requires very little effort to implement and virtually no ongoing support. PhoneFactor offers instant integration with all leading business systems and synchronizes with AD and LDAP servers for centralized user management. Easy, automated self-service options are available through the phone and web, which helps to significantly minimize overhead.

## Conclusion

When you look at the Total Cost of Ownership for an authentication solution, it's critical to look for solutions that have tools and systems that are going to help minimize the amount of overhead for your IT department. This cost can add up to a considerable portion of your Total Cost of Ownership, creating a significant impact on your Return On Investment.

For this and many other reasons, awareness and adoption of phone-based authentication are growing at an astounding rate. As companies try to defend against current and future threats, they are looking to PhoneFactor to provide the increased out-of-band security they need at a pricepoint that delivers a high return on their investment.