

DocuSign is an effective tool to combat ID Theft and possible loss of Customer Information

Introduction

According to recent FTC surveys and surveys by other firms, the predominant number of ID theft occurrences happen with paper records, and not with electronic records. In fact, in 2003, paper-records including credit cards, checking accounts and other forms of paper accounted for 86% of the misuse, while only 3% of the fraud was based on Internet activity. This is surprising because most of the ID theft reported in the news is electronic in nature. Of course, it is more interesting to report on electronic ID theft than lost wallets and lost documents stolen from dumpsters.

This document discusses how businesses who wish to reduce their chance of ID Theft should move to secure online systems such as DocuSign. This move can reduce the risk of catastrophic loss due to ID Theft or loss of sensitive customer data. This is especially important to companies seeking to establish policies which uphold the Gramm-Leach-Bliley Safeguards rule.

According to the FTC, in 2003 ID Theft totaled more than \$10B and affected millions of consumers. Those figures grew dramatically in 2004. The bulk of this ID theft took place through compromised paper documents such as paper mail or trash. Of the online ID theft, very little was due to fraudulent email. This is surprising given that more than 75% of US households have access to the internet, and most businesses do as well. In addition, reported losses from ID theft of paper records is much higher than losses due to compromised electronic records because consumers discover online ID theft faster.

Some of the more common modes of ID theft are as follows:

1. **Stolen wallet, checkbook or credit card** - a common theft of ID
2. **Stolen mail, Friends or relatives have access to documents**– The thief simply opens your mailbox before you do! From this, they can find bank statements, service accounts, credit card numbers, and other information which makes it very easy to open accounts in your name, etc.
3. **Stolen trash/internal employee**– throwing out bank statements and other documents without shredding them is another leading cause of ID Theft
4. **Lost or Misplaced files** – having a page drop out of a folder on the way to your car, or a fax page falling down on the floor with important information can lead to ID theft. If you manage lots of paper, keep it all together can be a challenge.

Business Impact of ID or Customer data Loss

Any business who manages customer information must keep control of all the customer information they possess. According to section 6801 of the Gramm-Leach-Bliley Act, companies who manage or store financial information about their customers MUST take steps to:

- (1) insure the security and confidentiality of customer records and information;*
- (2) protect against any anticipated threats or hazards to the security or integrity of such records; and*
- (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.*

Companies found to not be taking effective steps in protecting their customer's information can be levied substantial fines and penalties. As part of a nationwide compliance sweep, the Federal Trade Commission has charged two mortgage companies with violating the agency's Gramm-Leach-Bliley (GLB) Safeguards Rule by not having reasonable protections for customers' sensitive personal and financial information. In an administrative action filed against Nationwide Mortgage Group, Inc. (Nationwide) and its president John D. Eubank, the FTC alleged that the Fairfax, Virginia-based mortgage broker failed to implement safeguards to protect its customers' names, social security numbers, credit histories, bank account numbers, income tax returns, and other sensitive financial information. Sunbelt Lending Services, Inc. (Sunbelt), a subsidiary of Cendant Mortgage Corporation with headquarters in Clearwater, Florida, has agreed to settle similar FTC charges. The settlement with Sunbelt will bar future violations of the Safeguards Rule and require biannual audits of Sunbelt's information security program by a qualified, independent professional for 10 years. These are the FTC's first cases enforcing the Safeguards Rule.

The Safeguards Rule, which implements the security requirements of the GLB Act, requires financial institutions to have reasonable policies and procedures to ensure the security and confidentiality of customer information. The "financial institutions" covered by the Rule include not only lenders and other traditional financial institutions, but also companies providing many other types of financial products and services to consumers.

Simply moving away from paper records to electronic management is not enough to remove all risks of data loss, as still a full 11% of ID Theft happens to electronic records. The most common ID Theft modes with electronic records are:

1. **Email theft** – users who send documents and attachments via non-secured email accounts or 'free' email services may be intercepted and attachments stripped off. Since most email is sent over unsecured lines (not using SSL) this is an area of vulnerability. Most people do not realize that the sensitive attachments they send along can be seen.

2. **Incidental Storage** – when an email attachment is delivered, the file is stored in a temporary file on the PC. A hacker who has access to the PC can easily find past attachments and steal the data.
3. **Easily discovered passwords** – many users do not create passwords that are hard to guess. For example, many users keep a password as simply 'password', number one on the list of passwords guessed by hackers. This is followed by passwords like '1111', or '12345..'.
4. **"Phishing"** – fake emails are sent to a recipient and they unknowingly click on the link and enter in their information to a fake site, which steals their password and access.

How DocuSign Improves Security

Using electronic tools to reduce chance of data theft is an imperative. Learning from the failures of the electronic systems such as email and weak passwords allows companies to form strong policies. One such move is to DocuSign for managing the communication of sensitive information rather than using paper or less secure electronic means. The benefits of DocuSign are as follows:

1. By moving from paper delivery and storage of sensitive information, most of all ID Theft sources can be eliminated. Using DocuSign rather than creating and moving paper records is not only cost effective, it is much more secure.
2. By using DocuSign to send sensitive notices and information to your customers, email attachment theft can be eliminated. Because DocuSign utilizes an SSL link to send documents directly from your computer system to the DocuSign repository they cannot be intercepted.
3. Once the documents are deposited into DocuSign, they are made tamperproof, and they are encrypted using RSA AES encryption. This is the highest form of security that can be applied to your documents.
4. For signatures, DocuSign creates a secure and industry leading process which has been evaluated by leading law firms, and is in widespread use.
5. For secure delivery of documents not requiring a signature, DocuSign provides 'Certified Delivery which is half the cost of documents sent for signature – a highly cost effective way to secure your information.
6. With DocuSign, valuable customer information is NEVER moved outside a non-controlled environment like a mail box, or an email attachment. What's more, the recipient must authenticate to access the record.

Summary

Companies or individuals concerned about ID Theft or securing customer information should strongly consider policies and workflows that leverage the secure DocuSign Online Signing Service. Whether for documents needing a signature, or for secure transmission of customer information, DocuSign is one of the most effective tools available to combat ID Theft and loss of sensitive information.

About DocuSign

DocuSign offers an electronic signature service that provides the simplicity, speed and security required to deliver, sign and store documents. Designed from the ground up for business-class usage, this service integrates the technical infrastructure and legal compliance needed to operate an end-to-end signing service. DocuSign customers span a variety of industries and range from the largest corporations to the smallest branch offices. DocuSign, Inc. is a privately held company based in Seattle, Washington.