WHITEPAPER

7 Ways your Fax Machine is Putting You at Risk for Identity Theft

How is your company protecting private information in everyday transactions?

This whitepaper is published by DPD International, makers of the popular GoldFax network faxing solution. For more information visit: www.GoldFax.com.

GoldFax

DPD INTERNATIONAL

Security is a common threat to every organization, no matter what industry, size, location or type of business. Doing business means communicating and transferring confidential information and critical data. Billing information, Social Security numbers, Doctor Prescriptions, credit card numbers, personal information, etc. is ordinary content being exchanged every day - all of which would be detrimental if captured by the wrong hands. Most companies have some type of security measures in action ***but few consider the perils of an unsecured fax system***. Organizations relying on unsecure faxing are opening up big doors for data and identities to be stolen in the blink of an eye. This document is designed to help you identify your fax security risks and recommend ways you can prevent Identity theft.

Risk Exposures

1. **Fax device location:**

Where are your fax machines located? In an easily accessible location? A hallway for convenience, a room without a door, at the front desk, or in an open office group? A fax machine sitting in the open not only makes it easy for employees to access but also for wandering eyes to notice as they pass by. Having confidential information easily seen in an area accessible to a public eye is a huge security exposure.

Installing external security, locked doors, card I.Ds, finger scans, etc. is the wrong solution. Plenty of curious eyes can still make their way to private documents on a fax machine. The potential for critical and personal information to be seen is very high.

You not only risk information leakage but also **reputations, licenses, and the likelihood of being hit with a lawsuit or heavy fine**.

- **HIPPA** requires personal security and confidentiality provisions for patients. An employee or ex-employee can walk by a fax machine and seize medical test results or prescriptions containing personal information paving the way for a lawsuit.
- **HR** regulations require employee and customer information and history be kept securely private. A guest walking back to an office for a meeting can easily glance at a just received fax document, exposing social security numbers and personal bank reports of an employee.
- A delivery person comes in to deliver food for the office and conveniently picks up credit card numbers and a name from a faxed order that is waiting to be retrieved. They leave with the account details of one of your customers.

2. Fax Content:

Content sent via a fax can be anything - billing information, social security numbers, account access codes, license keys, passwords, patient reports, financial reports, personal history, confidential agreements, etc. all with names and information easy for stealing an identity. The information could be concerning customers, vendors, dealers, etc., so **you're not only threatening your own identity and security but are also responsible for your business partner's confidential data**.

- A **patient's history** report sent from a Doctor can expose private information and personal details that violates HIPPA regulations.
- An **insurance claim** from a person in the public eye is spotted and leaked to the press damaging personal and professional reputation and creating a media storm.
- A **faxed order** can contain an entire identity on it: name, phone number, credit card number, security code, billing address, etc. An office visitor that picks up and copies the information from a fax now has the identity of a customer.
- An **application for employment** or service with contact information is viewed by another employee who has a previous history with the applicant. The employee tosses the fax out or tampers information on the application before it is delivered to HR.

3. Off Hour Access:

Normal business hours and days are more easily monitored. Any suspicious activity may be noticed. However, many fax pages can be left sitting around for minutes, hours, even days.

Doing business internationally means adjusting hours and times to be available to both send and receive faxes.

Extending work hours and implementing extra security measures such as access codes, finger scans and passwords, still leave the basic risk exposure.

Physical security measures do not protect you enough.

Disgruntled employees, competitors, and unaffiliated persons are still allowed access (i.e. cleaning crew, delivery personnel, building owners, etc.) to the fax devices. Anything coming in after hours is easily grabbed or copied. An soon to leave employee can also send out confidential documents and put the originals back in the files.

- An order for a shipment is placed and faxed from a Colorado business to a company in Maryland. The fax, complete with credit card information, billing address and name, is received late at night after standard business hours. The **cleaning crew** arrives for their normal cleaning and picks up the fax and identity.
- A detailed financial history faxed from an international sister company **arrives early in the morning**. The first employee into the office reads through it before sending their fax and gains confidential company information – for example, a reduction in force, new potential customer, financing details, promotions, etc.
- A medical claim faxed while the intended recipient is **at lunch**, exposes potentially damaging information to anyone who uses the fax machine.

4. Document Size:

While many faxes are typically a few pages, several are often tens of pages long. Faxing a long or detailed document can take several minutes and usually, the intended recipients are **not stationed by a fax machine receiving each fax page as it comes in leaving an easy gap in security for a document to be tampered.**

- **Fax piggy backing**. A one page fax can get mixed in with other longer faxed documents that have come in and picked up by another employee expecting a fax.
- **Blackouts**. Dense images on documents will slow down the processing and interfere with incoming and outgoing faxes.
- **Unintended theft**. A person places a lengthy document to be faxed and leaves the room. After the document has faxed, another document is received and placed into the same pile. The person comes back to retrieve their sent document and picks up the received personal fax as well.
- **Hmm – missing a page**. A long insurance claim is received and waiting to be picked up by an adjuster. An office visitor walking by picks up one of the pages with critical information, leaving the rest of the document there so the recipient may not notice the missing piece.

5. Shared Fax Numbers:

Does each employee have a confidential fax number? Fax machines are expensive including the costs of toner, paper and maintenance. One machine typically serves several people within your company or organization.

More people using a machine means the higher the risk of exposure and the easier the potential to steal an identity.

Having several employees utilizing a single fax machine creates more opportunities for mix-ups, lost documents and tampered data.

- A **health premium** request is faxed by an employee and another individual going to use the fax machine, obtains of the premium request fax as well along with private information and the claim.

- The **CFO's medical test** is faxed to the office and an intern picks up the fax they were waiting for and grabs the CFO's fax – on purpose or by accident, exposing private information and violating HIPAA regulation that protects patient's information.
- You leave a large document to be faxed on the fax machine and walk away as the document gets scanned in. Another person comes by, **tampers the document**, and places it back on the machine to be faxed.

6. Evidence of Receipt:

How do you prove that your private and confidential information that was faxed was securely received?

Your company might be secure but what about the locations you are sending it to?

Are they exercising precautions? Do they share a central fax machine that is easily accessible? Just because a document on your end has reached a dialed number, does not guarantee that the intended recipient was eagerly waiting on the other side of the fax to accept it.

- A purchase order faxed over with your **company credit card** and billing information reaches the intended destination but not the intended receiver. An unknown person now has your company billing information and identity.
- A healthcare administrator faxes over **medical exam results** and a critical prescription over to an office before leaving for vacation. The fax is accidently picked up off the machine and the patient never receives it.
- An **urgent renewal** is returned via fax with agreement to a deal but the fax is claimed to have never been received so the deal is lost.
- A **contract** for a piece of real estate is signed and faxed over but alleged to never have been received. The space is sold to another firm. You have no proof of what was faxed.

7. History Report – Audit Trail:

Do you have an audit trail for corporate communications? Most fax machines typically maintain a short history of sent or received faxes – phone number, pages, and date/time that are printed automatically or with the press of a button.

- You send a **confidential medial report** to a celebrity patient exposing personal health information. A nurse later reviews the sent faxes and gains personal information about the celebrity which she passes along to news and public magazines. Not only do you face heavy fines under HIPAA but also legal action from the patient.

*HIPAA violation leads to **prison term** for surgeon who peeked at celebrities' records*

- Your corporate office demands a critical financial report be faxed by 12:00pm. You fax the report but headquarters doesn't receive it until late that night – their fax machine was busy or out of service. Assuming you sent the report late with no evidence on the time sent, **your job is terminated**.
- An employee claims to have faxed a customer's insurance report last week but the customer is upset because he **never received the document**. The customer cancels their contract after finding no records of sent faxes to the customer.
- **Insider information** about a merger is leaked by an employee who sees some fax pages and corporate officers are facing huge fines because it was in a quiet period.
- You send a document with private accounting data. Shortly after you leave the fax machine, another employee **resends the sent fax to an additional number**, sending off confidential data without your knowledge.

There are endless scenarios that can be explained regarding the lack of security in a standard fax machine and the effects on an organization. But these cases are true and the chances of them happening in your organization are high.

Is your organization capable of handling the aftermath of lost contracts, identity theft, lawsuits, HIPPA fines and bankruptcy?

The risk is not worth it, especially when there are simple steps you can take to increase your security and protect your identity.

What can you do?

1. **Physical Security:**

   Many organizations think they have or can take steps to ensure the security of their offices by installing physical security measures such as door or cabinet locks, proximity readers, finger print scans, retinal scans, and metal detection and x-ray machines. However, while these tactics are good precautions, they don't adequately reduce the risk. **The internal risk still exists**. How many people know the code or can gain access?

- An employee, entitled to access a fax machine, could easily pick up a **private Doctor note** left on the fax machine unveiling private information about another employee.
- An office worker could see where card keys are stored and easily pick up the key and send a **fax with confidential data** using another employee's ID.
- Different departments within the same organization still have the ability to see information coming in. A **late night fax** could be retrieved by an unintended person the following morning.

Installing physical security does not eliminate the main problem which is confidential and private information sitting out in the open.

2. **Data Security:**

   Computers store massive amounts of data, a gold mine for computer hackers and identity thieves. Organizations and companies often install firewalls, virus protection, and other data security systems to protect information received from customers, employees and competitors. What about the confidential data printed out to be transmitted via fax?

   As long as your information is being printed

   so it can be faxed, it is at risk for being copied, stolen or lost.

3. **Policies:**

   Establishing company guidelines or organizational rules helps outline security measures and precautions each employee should make to ensure security of private information. Policies such as *lock up all documents*, *do not write down passwords*, *do not open email from unknown sender* etc. all contribute to exercising more safety measures however does not decrease the main risk.

What or who is monitoring that all employees are following policy rules?

These actions can all help your organization develop stricter standards and precautions, but the **risks still exist.**

The Secured Software Solution

Fax software is the most effective and efficient way to increase security for your organization. Employing easy to use network faxing software, like GoldFax, enables an organization and its users to avoid costly mistakes and fines that would result from lawsuits regarding lost information, tampered evidence, stolen identities and fines.

How Fax Software Works to keep you Secure:

Fax software **eliminates the security threats**. Instead of sending and receiving faxes from an open fax machine, GoldFax faxes straight from a user's desktop, mobile device or MFP. The fax from email capability removes the risks of leaving a document on the machine for any wandering eyes to see or eager hands to take. This also includes incoming faxes which can be sent directly to the intended recipient's inbox email account. In doing so, confidential information, pertinent data and critical reports are delivered to the intended recipient with a proof of receipt and safekeeping. Faxed documents converted into PDFs and other formats can now be archived, printed or forwarded to the proper person electronically. This individual delivery removes the threat of information being received in a "public area" where there is the risk of tampering, loss, and no proof of secured delivery.

Every organization has some type of regulatory mandate that must be met whether it is HIPAA, Sarbanes Oxley, FINRA or Gramm Leach Bliley. A Fax software solution such as GoldFax, facilitates organizations in meeting the heightened compliance expectations to secure and retain information.

- **Electronically records actions** and exchanges of email faxes- removing the risk of stolen or tampered hard copies.
- Programs routine tracking features to **satisfy audit** trail requirements.
- Notifies of **proof of delivery** with a receipt for sent and received documents.
- Allows **archiving** capabilities that automatically record and store information in desired folders, making information easily available for auditing purposes.
- **Secured storage** of confidential documents.

Failure to follow compliance regulations not only puts your organization at risk, but also invites heavy regulation fines. Are you willing to pay thousands of dollars for violating regulations?

Find out if your organization is compliant: www.goldfax.com/IndustryRegulations

Protect Identity Theft: Secure your Fax Environment

In the type of business world we live in today, it is crucial to exercise security and precautions. Be proactive and stop any opportunity for your employees, your customers, your partners' and your identity and information to be stolen.

GoldFax is a high performing fax software solution that scales to any business size-delivering powerful, reliable, and affordable solutions that secure your fax environment and keep you in compliance. GoldFax software lets you send and receive faxes from any desktop application, removing the threat associated with manual faxing that leaves documents out in the open.

Offering fax by email, your confidential information is protected from outside eyes and delivered through a secure network. Documents are securely sent and received with notifications and proof that delivery was successful.

See how GoldFax can increase your security and efficiency by visiting: www.goldfax.com.