# NET SatisFAXtion Security Whitepaper

## Fax is Secure

By the very nature of fax communications, it is secure. Any fax device communicates with other fax devices with Group III or Group IV fax protocol. These fax protocols are designed to only send image data in one of the supported image or rather compression methods: Group III, Group IV, JBIG and JPEG. Think of this as simply sending from one fax machine to another. The only thing that can pass between the two fax machines is the image of the paper that was scanned. The only information that the receiving fax machine can output is a printout of the received fax image. There is no mechanism with Group III Group IV fax protocol to allow foreign or dangerous information to pass.

## The Safest Way to Send a Message

People send documents as attachments via Internet email every day, without realizing the security and reliability risks they are taking. With the events of the past 18 months, many individuals and businesses have begun to regard both postal mail and e-mail with heightened suspicion. In light of these events, many businesses and government organizations, including the United States Congress, have turned to fax as a primary method for communicating.

Unlike an e-mail attachment, a fax document is an image file, *NOT AN EDITABLE FILE*. No one can alter the original itself to embed another program within it, meaning a fax can never cause a computer virus or worm to invade your network.

FaxBack makes it easy to add network fax capabilities to Windows and Outlook clients with its family of NET SatisFAXtion products. NET SatisFAXtion allows companies to quickly and reliably transmit time-sensitive, confidential documents from desktops or mission-critical applications within your enterprise.

## How Secure is Your Fax Machine?

Sending faxes containing confidential information can be risky when the security on the receiving end is in question. Think about how often you have accidentally seen a confidential fax when sending or retrieving another fax. If the fax machine is in a public location, it is not secure. To counter this risk, many companies, departments and workgroups are deploying network fax servers, like NET SatisFAXtion to ensure that confidential faxes are directed to secure email addresses and fax numbers. NET SatisFAXtion's inbound routing options support several secure methods including "cover page only" routing (only the first page of the fax can be viewed for routing purposes) as well as DID and DNIS (faxes are automatically directed to a private mailbox for viewing).

## Fax Security with Class1/Class2 Fax Modems

In the case when either the sending or receiving (or both for) fax device is a computer with a Class1/Class2 fax modem the connection is still secure. The receiving fax device, a Class1/Class2 fax modem in this case, is configured by the software drivers from FaxBack to only communicate with Group III or Group IV fax devices using the fax protocol. When the fax modem answers an incoming call from a remote device that is not a fax device, it will hang up the call. There is no possible way for the receiving fax modem to deviate from this action. If the receiving fax modem that is set by the software drivers to be a fax device it will only communicate via Group III or Group IV fax protocol. Any other data stream or handshaking will cause the connection to be cut off.

A fax modem can only be configured to answer from a single driver source. NET SatisFAXtion's Class1/Class2 fax drivers will configure the fax modem to only answer in fax mode. As long as the physical system is secure, the connection into your office, even thought it is through a phone line is secure.

## Network Security

NET SatisFAXtion relies on your company's internal network infrastructure security. This means that any internal access to the information on the fax server system is controlled by your own local network security.

## Client Security

There are various clients that can connect to the NET SatisFAXtion fax server to send faxes. These include: FAXability, WinFax PRO and any e-mail client. The connection between these clients and the fax server relies on your network infrastructure to be secure. The connection for remote access is also secure because of the connection infrastructure that is in place. Your e-mail system and/or ISP is responsible for the secure connection for e-mail clients. If you are using NET SatisFAXtion's FAXability fax client from a remote site, the connection security is handled by the web server that is hosting the FAXability fax client. This can be normal web access or a secure SSL connection.

All client access to the NET SatisFAXtion fax server requires a username and password for both FAXability and WinFax PRO. Users using their e-mail client gain access via their e-mail logon. NET SatisFAXtion can be setup to limit which users on your e-mail system have access to the NET SatisFAXtion fax server to send or receive faxes.

## Information Security

Any confidential fax information that is either sent or received by the NET SatisFAXtion fax server relies on the following aspects for security: local physical system security, network security, remote connection security, client access security and client workstation security.

## HIPAA

NET SatisFAXtion's line of fax server solutions enable organizations to deliver confidential documents electronically in accordance with HIPAA regulations. A NET SatisFAXtion fax server can automatically route an incoming fax directly to the recipient's desktop, a network folder or to a database, depending on the fax number used by the sender. The fax message can also be delivered as a TIF or PDF file attachment inside a standard email message. In addition, incoming faxes that are directed to a "postmaster" or "general" inbox for manual routing can be set-up to have only the "cover page" viewed, allowing confidential information to stay private.

The HIPPA regulations apply to specified health care industry entities: health care providers, insurance plans and information clearinghouses. The regulations also require these covered entities to assure that their "business associates" also contract with them to comply with HIPAA.

In 1996, with the passage of the Health Insurance Portability and Accountability Act (HIPAA), the federal government took the lead in drafting rules to govern the secure transmission and storage of electronic health records. The final rules governing the privacy of medical records were issued by the US Department of Health and Human Services (HHS) on December 20, 2000. The point of HIPAA was to reduce the administrative costs and burdens of healthcare by establishing uniform standards for the transmission of health care data and facilitating health care transactions. The rules apply to both oral and written communications, and include information related to the payment for healthcare as well as medical records themselves. In essence, protected health information is any data relating to an identifiable individual's physical or mental health, the provision of a person's healthcare, or the payment for that healthcare. Anonymous medical data is not covered under the rule, but a medical record must be scrubbed of all individualized data before it can be considered anonymous. The new rules were originally meant to cover computerized records, but the final rules also cover paper records, emails, faxes, voice mail messages and even telephone and other oral conversations.

## Summary

For more than twenty years FaxBack has been a leading fax messaging company with solutions that radically simplify the way organizations communicate. We provide award-winning network fax servers, fax-on-demand, broadcasting and web-to-fax solutions that streamline information processes, get time-sensitive information into the hands of your audience faster than ever before while reducing the cost of doing business.

First introduced in 1990, NET SatisFAXtion is an award-winning fax server with tens of thousands of fax servers installed in North America alone. Designed for organizations that need to control and simplify their fax communications, it is enjoyed by thousands of global organizations including AT&T, Arco, Bank of America, Compaq, Kaiser Permanente, Kodak, NEC, Sherwin-Williams and Wells Fargo. Countless other organizations in nearly every industry from real estate to manufacturing and travel to education and healthcare trust FaxBack and NET SatisFAXtion for their fax communications needs.

## More Info

| | |
|---|---|
| Voice: | (503) 597-5350 |
| Fax: | (503) 597-5399 |
| Web: | http://www.faxback.com |
| **E-mail:** | info@faxback.com |

SEE ALSO the related white paper on the FaxBack Voice Server security named:

"FaxBack Voice Server Security"

# Voice Server Security Whitepaper

## IVR Voice Ports are Secure

IVR voice ports are secure. They do not by their nature allow any type of modem communication. The capabilities of these ports do not extend beyond these functions:

- Detect ring and go off hook
- Play audio voice prompts
- Accept DTMF touch tone entries
- Record audio voice prompts (supervisor mode)

As long as the physical system is secure, the connection into your office, even thought it is through a phone line is secure.

## Voice hardware Security

Analog and digital voice hardware contains no circuitry for modem or LAN communications. It operates solely when connected to a telephony circuit via audio frequency communications. The voice hardware supported by the FaxBack Voice Server includes cards from Intel / Dialogic and PIKA Technologies. All have been tested and verified for telephony-only security.

## Network Security

The Voice Server relies on your company's internal network infrastructure security. This means that any internal access to the information on the fax server system is controlled by your own local network security.

## Information Security

Any confidential information that is either sent or received by the Voice Server relies on the following aspects for security: local physical system security, network security, and remote connection security.

## Summary

The voice ports on the FaxBack Voice Server do connect to the outside world via a telephone line. However, the connection they enable is voice-only. It is simply not a "hackable" connection.

SEE ALSO the related white paper on NET SatisFAXtion fax server security named:

"NET SatisFAXtion Security"

FaxBack