



## Wireless Devices on Trading Floors - Regulatory Compliance Risks



[www.airpatrolcorp.com](http://www.airpatrolcorp.com)

## I. Introduction

Without proper surveillance on trading floors of wireless equipment, such as cellular phones and 802.11 wireless devices, firms are in danger of violating regulatory policies and encountering damaging consequences of rogue trading activity. Notorious cases, such as the 1995 Barings Bank collapse caused by one rogue derivatives trader, as well as the more recent debacles, such as the Société Générale loss of over \$7 billion due to a renegade trader executing elaborate, fictitious transactions with access to other employees' emails, demonstrate the severity of the rogue trader problem in an environment where proper surveillance is not taking place.

In addition to the financial losses caused by the rogue trading event itself, the penalties for firm violation of regulations can include:

- multimillion dollar fines;
- criminal penalties for executives, as well as for traders;
- loss of exchange listing, trader licenses and registration;
- censures or restriction of business lines;
- loss of D&O insurance;
- outside directors' liability above D&O insurance limits;
- shareholder lawsuits; and
- loss of investor confidence.

## Wireless Surveillance – The Solution

While many financial institutions today have wired systems in place to monitor compliance on their trading floors, if traders have alternative wireless means of communication which are not monitored, then the value of that wired surveillance can be severely diminished, if not rendered moot. A wireless surveillance system on a trading floor will drive all electronic communications back to the wired network, so that the existing wired surveillance systems can track the true value of the transactions taking place. *Such a surveillance system would greatly assist a firm in complying with regulatory requirements, as well as in preventing insider trading, fraud and other nefarious activity on a trading.*

Amid heightened regulatory scrutiny, as well as the current challenging financial environment, it is now more pressing than ever for firms to ensure regulatory compliance and prevention of rogue trader activity. To understand the complexities, it is helpful to review some of the key applicable regulations.

## II. A Regulatory Review

### SEC Rules

The Securities and Exchange Commission (SEC) Rules require firms/traders to create specific records relating to each security transaction, as well as information regarding its customers, employees and overall business.<sup>1</sup> Orders can be generated by electronic order management systems, but all such transactions must be recorded. Orders can not be left on voicemail.<sup>2</sup>

### NYSE OTS

The New York Stock Exchange (NYSE) Order Tracking System (OTS) requires all brokerage firms that enter listed orders to the marketplace to maintain records of all activities in the lifecycle of the order, including when the order was received or generated, canceled or executed. All listed order events must be documented and include time-stamps and order detail.<sup>3</sup>

### FINRA OATS

The Financial Industry Regulatory Authority (FINRA) Order Audit Trail System (OATS) requires all brokerage firms that enter over-the-counter (OTC) orders to the marketplace to record the details of such orders, including time-stamps and order details. At the end of each business day, each firm must transmit an audit trail, including order/execution flow to FINRA, including the following order types: New Orders, Cancels, Cancel/Replaces and Executions.

### CFTC

The Commodity Futures Trading Commission (CFTC) Division of Enforcement investigates and prosecutes alleged violations of the Commodity Exchange Act and Commission regulations.

### SOX

If the firm is publicly listed in the US or under the jurisdiction of the SEC, The Sarbanes-Oxley Act of 2002 (SOX) applies to the firm, as well as to the accounting firms that provides with auditing services. *Although SOX does not on its face, specifically address IT security, a deeper look into the requirements reveals that SOX very much involves IT security of financial information, including information transferred within the firm – such as on the trading floor.*

---

<sup>1</sup> SEC Rules 17a-3 and 17a-4

<sup>2</sup> Rule 17a-4 mandates that the records be preserved for several years - the number of years is dependant upon the type of record and transaction, while Rule 21(a) gives the SEC the authority and discretion to investigate violations of any SEC provisions, along with numerous other related rules and regulations.

<sup>3</sup> Upon request from the NYSE, firms must query their databases and transmit their OTS files to the NYSE. Firms must maintain a database of activity for a number of years.

The relevant portions of the Act for these purposes require the firm officers to certify that:

- they have reviewed the annual financial reports;
- the information is complete, accurate and not misleading;
- internal disclosure controls are in place to ensure accurate financial reporting; and
- such controls are effective (documented evidence).<sup>4</sup>

A registered public accounting firm shall, in the same report, validate and report on the assessment of the effectiveness of the internal control structure and the financial reporting procedures.

### **III. Summary of Regulatory Impact on Trading Floor Surveillance**

As IT is integral to the financial accounting, tracking and reporting of financial information of firms, it follows that a firm should ensure that it has a secure wireless threat management system in place on the trading floor to capture all relevant financial data. The majority of today's mobile phones and wireless devices have built-in cameras, data storage and transfer capabilities that introduce new fraud opportunities and threaten the security of confidential information and can be used to circumvent IT policies, such as call recording requirements, by the ability to make calls, and/or send e-mails, texts or even Instant Messages.

Detecting - and more importantly, locating and stopping - the use of cellular phones, as well as wireless devices, helps firms protect against unauthorized communications on trading floors. If a trading floor does not have a surveillance system in place to detect cellular and wireless devices, it cannot ensure that it is capturing all financial data, as is required by the regulators, nor can it ensure that rogue trading, fraud and other illegal activity is not taking place outside the wired system.

### **IV. Regulators Crack Down on Insider Trading and Fraud**

The SEC is aggressively combating fraud and market manipulation through investigation and enforcement actions. *Notably, recent investigations have involved the trader's use of wireless equipment on the trading floor to communicate the insider or fraudulent information.*

#### **SEC, NYSE Regulation and FINRA Investigations**

On September 19, 1008, the SEC announced a broad expansion of its ongoing investigation into possible market manipulation in the shares of certain financial institutions. Investigators

---

<sup>4</sup> Sections 302,404.

from NYSE Regulation and FINRA are conducting a parallel, yet separate, investigation in coordination with the SEC, which includes on-site visits to various firms.

**Among recent actions taken by the SEC are those which involve the use of e-mail and/or electronic Instant Messaging:**

In 2007 and 2008, a sole trader with Société Générale had access to the **e-mail** of some of the firm's engineers, which assisted him in carrying out the infamous \$7 billion plus fraud.

In April 2008, a landmark enforcement action for securities fraud and market manipulation was brought against a Wall Street trader who spread false rumors, by **Instant Messaging** traders at brokerage houses and others, regarding The Blackstone Group's acquisition of Alliance Data Systems (ADS), while he was selling ADS short. The media obtained the news, as well.

In September 2008, two Wall Street brokers were charged with defrauding their customers when making more than \$1 billion in unauthorized purchases by **sending or directing their sales assistants to send e-mail confirmations** in which the terms "St. Loan" or "Education" were added to the names of non-student loan securities purchased for the customers.

## V. IT Risks on Trading Floors Threatening Compliance with Regulatory Policies

- **Policy Established from the Top:** A ban on cellular phones and wireless equipment should be established from the top executives, as an example to regulators of the firm's extensive efforts toward compliance and tough stance against rogue trading.
- **The Myth of the "Honor Policy":** If the firm's policy banning wireless equipment on the trading floor is an "honor policy", it will not likely be "honored" by those prone to committing insider trading and fraud – electronic surveillance is necessary.
- **By Passing the Recording System:** If the firm has a policy of recording all trades on a wired telephone, but does not have a policy or surveillance preventing traders from using wireless devices on the floor, a recording policy is moot. This is fertile ground for rogue traders.
- **The Need for Tracking Patterns of Behavior:** It is important that traders use the firm's wired systems in order for the firm to ensure accurate financial reporting and to be able to detect unusual activities and behavior – providing an early warning system to the firm of possible illegal events, while remaining in compliance with the regulatory obligations.
- **The Fallacy in the "Personal Emergency" Need for Devices:** Traders can make and receive emergency calls by being alerted by a guard and leaving the Trading Floor. Certainly, a trader can make a call containing insider or fraudulent information by leaving the trading floor, but having a no wireless policy and electronic surveillance will assist the firm in arguing that it has complied with the regulations requiring internal controls.

- **A Condition of Employment:** If the firm makes the ban on cellular phones and wireless equipment a condition of employment, it is one more way to demonstrate to regulators that it is taking steps to comply with regulations while attempting to prevent rogue trading activity. If a trader violates the policy, he could be subject to sanctions, suspension or termination, further deterring rogue trading activity.

## VI. AirPatrol Corporation's Solution

### AirPatrol Wireless Locator System (WLS)

In order to comply with the regulations, it is essential to have a surveillance system in place whereby the firm can determine immediately whether a cellular phone or wireless device is on and where it is located on the trading floor, so that its use can be stopped. AirPatrol's Wireless Locator System (WLS) provides the actionable intelligence network administrators need to confidently manage cellular phone and wireless device threats and enforce bans on these devices.



A detail from the Floor Plan console from AirPatrol's Wireless Locator System (WLS)

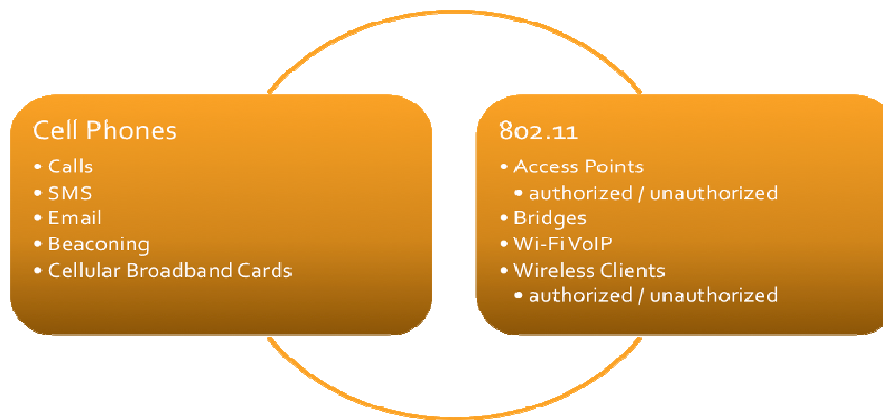
### Solution Overview

WLS provides the administrator with the ability to detect and accurately locate all cellular phones and wireless devices on the trading floor to an accuracy of 15 feet or better, at which time the administrator can take action to stop the transmission. WLS is the only solution known to the market today which:

- is capable of detecting both cellular phones and wireless equipment with one technological solution;
- is capable of detecting a cellular phone before a call is made (i.e. when the cellular phone is on, but is not in use); and
- is capable of detecting all messages sent by a cellular phones, (such as SMS messages and voice calls) as well as network infrastructure messages (such as when a cellular phone is turned on and registers with the network).

This revolutionary functionality allows security personnel to proactively respond to potential threats before any actual damage is done.

## Detect, Locate and deal with wireless threats to your security!



### Sensors

Sensors can be installed using a conventional wired or wireless Ethernet network. The inclusion of a second, pass through Ethernet interface in conjunction with the sensor's "Power over Ethernet" (PoE) capabilities enables the sensors to share existing network infrastructure and eliminates the requirement to install additional cabling and provision additional switch ports, dramatically reducing the complexity and cost of deployment.

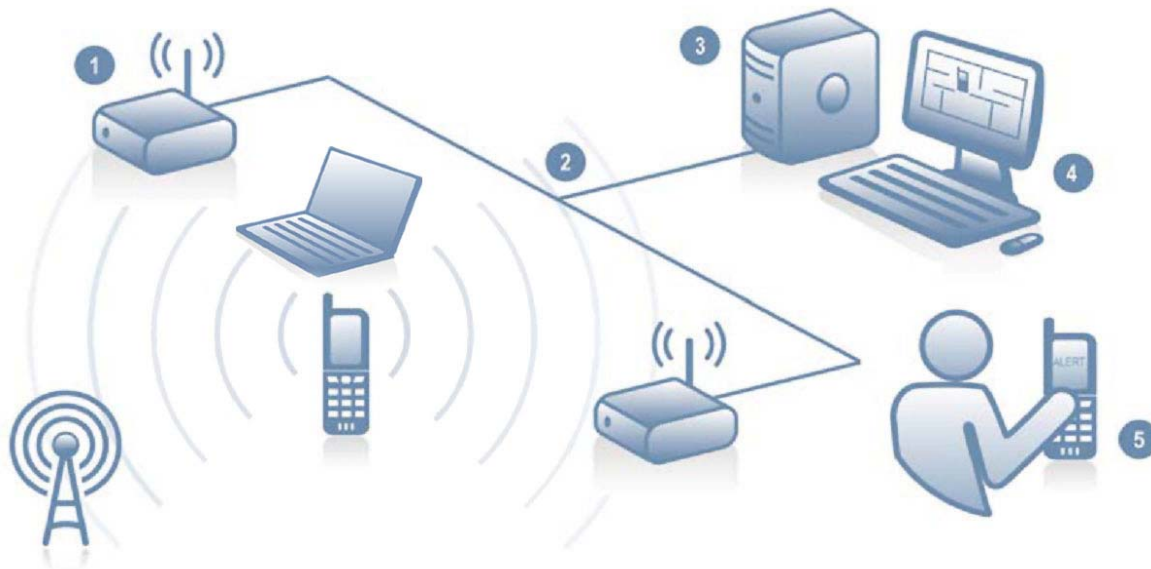
### Locating

The locations of all cellular phones and other wireless devices are displayed on the WLS Console in real-time. If the detected wireless device is registered with the organization, the name of the registered user can also be shown. In addition, alerts can be sent in multiple formats to multiple devices to notify security staff immediately whenever an unauthorized cellular phone is detected. Through the use of "alarm zones", your security personnel can also configure WLS to stand guard over a smaller region within a larger area. This can be extremely important when the region of interest is adjacent to a public area. In accordance with FCC rules, the system does not actively block any voice or text message communications. Instead it detects and locates the source, allowing security personnel to identify and respond to the security threats accordingly.

### Reporting

WLS contains an extremely rich set of customizable events, all of which can subsequently be used to generate customizable reports. Reports can be generated for each major subsection of event types (cellular phone detection, rogue wireless device detection, etc) and can be customized to include more or less detail in order to allow you to meet your regulatory requirements. WLS also contains the unique capability of being able to "replay" the events surrounding a particular security anomaly. Historical positioning data can be replayed forwards and backwards, at up to eight times normal speed.

## How It Works:



1. When a cellular phone beacons a cellular tower, initiates a voice call, or sends an SMS message, the sensors detect the activity. Wireless networking traffic is also detected by the sensor every time a wireless networking packet is sent over the airwaves.
2. The sensors relay the information over the network to the WLS server.
3. The WLS server analyzes the data from multiple sensors and determines the location of the cellular phone or wireless device.
4. The location of the wireless device and its details are then displayed on a facility floor plan within the WLS Floor Plan Console.
5. Details about the event are sent to any email-capable device such as a Blackberry/cellular phone, Network Control Center, etc.

Network administrators or security personnel are able to monitor, respond to, and resolve any issues in real-time.

Reports identifying any security policy violations can be generated. Historical playback of positioning data can be utilized to see what happened and when.

## WLS Key Differentiators

- 100% Dedicated Solution that is completely passive in nature
- Provides 24 x 7 monitoring and tracking of all cellular and 802.11 wireless devices – only system which can detect and locate both
- Easily installed, avoiding significant deployment costs
- Only system which can detect and locate a cellular phone which is on, but not currently in use
- Detects all types of cellular traffic, including SMS messages
- Detects all types of 802.11 a/b/g/pre-N devices.
- Rich set of Notification and Reporting Capabilities allowing for Forensic reporting in real time. Historical playback gives the ability to see exactly what happened and when.

## VII. Summary

Today's strict regulatory and turbulent financial environment, financial firms are under intense scrutiny regarding financial reporting, auditing and responsibility. It is now that firms must be particularly sensitive to the appropriate regulations to become or remain in compliance and to prevent nefarious rogue trading activity.

AirPatrol's WLS software provides the actionable intelligence network administrators need to confidently manage cellular phone and wireless threats and enforce bans on such devices on trading floors.

AirPatrol greatly simplifies and dramatically lowers the cost-of-deployment of cellular phone and wireless detection technologies to less than half of the cost of traditional solutions and enables sensor technology to be integrated into existing network infrastructure, rather than being deployed as a parallel network with a discrete overlay security strategy. Once deployed, administrators can manage the environment from a single easy-to-use console that is capable of concurrently displaying all cellular, 802.11 and broadband radio devices – and can detect, locate and stop the use of the unauthorized device before the damage is done.

## About AirPatrol Corporation

*AirPatrol brings real-world insight into the specific security risks faced by trading floors and financial institutions: AirPatrol Chairman, Mr. Bradley Rotter, has extensive experience on Wall Street as a Fixed Income Trader for EF Hutton, and as a Trader with the Chicago Board of Trade and the Chicago Mercantile Exchange.*

*As the most trusted authority on wireless threats to wired and wireless networks, AirPatrol Corporation delivers the security and network management capabilities today's businesses and government agencies require to solve the industry's most pressing wireless security and network management issues. By offering a comprehensive suite of wireless threat management solutions, AirPatrol enables entities to keep pace with the expanding requirements of a mobile world while complying with pertinent regulations and protecting communications, critical information, and IT infrastructure against present and future wireless threats. Customers and partners include leading network infrastructure and wireless vendors, Fortune 100 enterprises and high-profile government agencies around the globe.*

*For more information about the contents of this white paper, AirPatrol Corporation products or our company, please contact us at [info@airpatrolcorp.com](mailto:info@airpatrolcorp.com) or call us at +1-866-430-4227.*