

BIO KEY INTERNATIONAL INC  
Form 10KSB/A  
June 19, 2006

# U.S. SECURITIES AND EXCHANGE COMMISSION

WASHINGTON, D.C. 20549

## FORM 10-KSB/A

### Amendment No. 2

Annual Report Pursuant to Section 13 or 15(d)  
of the Securities Exchange Act of 1934  
For the Fiscal Year Ended December 31, 2005

Commission File Number 1-13463

## BIO-KEY INTERNATIONAL, INC.

(Name of small business issuer in its charter)

**DELAWARE**  
(State or other jurisdiction of  
Incorporation or organization)

**41-1741861**  
(IRS Employer  
Identification Number)

**3349 HIGHWAY 138, BUILDING D, SUITE B, WALL, NJ 07719**

(Address of Principal Executive Offices) (Zip Code)

**(732) 359-1100**

Issuer's telephone number, including area code.

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Exchange on which Registered
Common Stock, \$0.0001 par value per share	None

Securities registered under Section 12(g) of the Exchange Act

**None**

Check whether the issuer is not required to file reports pursuant to Section 13 or 15(d) of the Exchange Act.

Check whether the issuer (1) filed all reports required to be filed by Section 13 or 15(d) of the Exchange Act during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes  No

Edgar Filing: BIO KEY INTERNATIONAL INC - Form 10KSB/A

Check if there is no disclosure of delinquent filers in response to Item 405 of Regulation S-B contained in this form, and no disclosure will be contained, to the best of registrants knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-KSB or any amendment to this form 10-KSB.

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act).

Yes  No

State issuer s revenues for its most recent fiscal year: \$14,226,095

The aggregate market value of the voting and non-voting common equity held by non-affiliates of the registrant based on the closing sale price of the registrant common stock as reported on the OTC Bulletin Board on March 15, 2006 was \$23,132,637. The information provided shall in no way be construed as an admission that any person whose holdings are excluded from the figure is an affiliate or that any person whose holdings are included in the figure is not an affiliate, and any such admission is hereby disclaimed. The information provided is solely for the record keeping purposes of the Securities and Exchange Commission.

As of March 15, 2006, 48,036,983 shares of the registrant s common stock were outstanding.

Transitional Small Business Disclosure Formats (check one):

Yes  No

**EXPLANATORY NOTE**

This Amendment on Form 10-KSB/A constitutes Amendment No. 2 to the registrant's Annual Report on Form 10-KSB for the period ended December 31, 2005, which was originally filed with the Securities and Exchange Commission on March 30, 2006 (as amended, the Original Report). The purpose of this Amendment No. 2 is to amend the registrant's financial statements and management's discussion and analysis for restatements of the registrant's December 31, 2004 and 2005 annual financial statements as amended, and to provide further clarification under Item 8A (Controls and Procedures). The restatements are further explained in note B of the financial statements. Except as amended hereby, this Form 10-KSB/A does not amend, update or change any other information contained in the Original Report.

**DOCUMENTS INCORPORATED BY REFERENCE**

None.

**TABLE OF CONTENTS**

<u>PART I</u>		
<u>Item 1.</u>	<u>Description of Business</u>	1
<u>Item 2</u>	<u>Description of Property</u>	16
<u>Item 3</u>	<u>Legal Proceedings</u>	16
<u>Item 4</u>	<u>Submission of Matters to a Vote of Security Holders</u>	16
<u>PART II</u>		
<u>Item 5</u>	<u>Market for Common Equity and Related Stockholder Matters</u>	17
<u>Item 6</u>	<u>Management's Discussion and Analysis or Plan of Operation</u>	21
<u>Item 7</u>	<u>Financial Statements</u>	41
<u>Item 8</u>	<u>Changes in and Disagreements with Accountants on Accounting and Financial Disclosure</u>	42
<u>Item 8A</u>	<u>Controls and Procedures</u>	42
<u>Item 8B</u>	<u>Other Information</u>	42
<u>PART III</u>		
<u>Item 9</u>	<u>Directors, Executive Officers, Promoters and Control Persons;</u> <u>Compliance with Section 16(a) of the Exchange Act</u>	43
<u>Item 10</u>	<u>Executive Compensation</u>	45
<u>Item 11</u>	<u>Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters</u>	48
<u>Item 12</u>	<u>Certain Relationships and Related Transactions</u>	50
<u>Item 13</u>	<u>Exhibits</u>	51
<u>Item 14</u>	<u>Principal Accountant Fees and Services</u>	51
	<u>Signatures</u>	148

**PRIVATE SECURITIES LITIGATION REFORM ACT**

All statements other than statements of historical facts contained in this Annual Report on Form 10-KSB, including statements regarding our future financial position, business strategy and plans and objectives of management for future operations, are forward-looking statements. The words anticipate, believe, estimate, will, may, future, plan, intend and expect and similar expressions generally identify forward-looking statements. Although we believe our plans, intentions and expectations reflected in the forward-looking statements are reasonable, we cannot be sure they will be achieved. Actual results may differ materially from the forward-looking statements contained herein due to a number of factors. Many of these factors are set forth under the caption Risk Factors in Item I of this Annual Report and other filings with the Securities and Exchange Commission. These factors are not intended to represent a complete list of the general or specific factors that may affect us. It should be recognized that other factors, including general economic factors and business strategies, may be significant, presently or in the future. Except as required by law, we undertake no obligation to update any forward-looking statement, whether as a result of new information, future events or otherwise.



**PART I**

**ITEM 1. DESCRIPTION OF BUSINESS**

BIO-key International, Inc., a Delaware corporation ( the Company, BIO-key, we, or us ), was founded in 1993 to develop and market proprietary biometric technology and software solutions. Biometric technology is the science of analyzing specific human characteristics which are unique to each individual in order to identify a specific person from a broader population.

On March 30, 2004, BIO-key acquired Public Safety Group, Inc. (PSG), a privately held company that is a leader in wireless solutions for law enforcement and public safety markets. PSG's primary technology is PocketCop, a handheld solution that provides mobile officers, such as detectives who are not typically in their vehicles, a hand-held mobile information software solution.

On September 30, 2004, BIO-key completed a transaction with Aether Systems, Inc. to purchase its Mobile Government Division( Mobile Government or AMG ), a leading provider of wireless data solutions for use by public safety organizations, primarily state, local police, fire and rescue and emergency medical services organizations. The PacketCluster mobile information software is integrated with 50 separate State/NCIC databases, as well as other state, local and federal databases. Its open architecture and its published Application Programming Interface (API) make it easy to interface with a wide range of information sources. PacketCluster products deliver real-time information in seconds, freeing dispatchers to handle more pressing emergencies.

Effective January 1, 2005, BIO-key International, Inc., a Minnesota corporation ( Old BIO-key ), reincorporated in the State of Delaware. The reincorporation was effected pursuant to an Agreement and Plan of Merger (the Merger Agreement ) whereby Old BIO-key was merged with and into the Company, its wholly owned subsidiary, in order to reincorporate in the State of Delaware (the Reincorporation ). As a result of the Reincorporation, the legal domicile of the Company is now Delaware.

Pursuant to the Merger Agreement, at the effective time of the Reincorporation: (i) each outstanding share of Common Stock of Old BIO-key, \$0.01 par value per share, was automatically converted into one share of Common Stock, \$0.0001 par value per share, of the Company; (ii) each outstanding share of Series C 7% Convertible Preferred Stock of Old BIO-key, \$0.01 par value per share, was automatically converted into one share of Series A 7% Convertible Preferred Stock, \$0.0001 par value per share, of the Company, with such Series A 7% Convertible Preferred Stock containing substantially identical terms and conditions as the Series C 7% Convertible Preferred Stock of Old BIO-key; (iii) each option to purchase shares of Old BIO-key's Common Stock granted by Old BIO-key under any warrant, stock option plan or similar plan of Old BIO-key outstanding immediately before the Reincorporation was, by virtue of the Merger Agreement and without any action on the part of the holder thereof, converted into and become an option to purchase, upon the same terms and conditions, the same number of shares of the Company's Common Stock at an exercise price per share equal to the exercise price per share thereunder immediately before the Reincorporation; and (iv) each warrant, option or stock option plan of Old BIO-key was assumed by, and continues to be, a warrant, option or plan of the Company. Accordingly, as a result of the Reincorporation, the shareholders of Old BIO-key became shareholders of the Company, and Old BIO-key has been merged out of existence by operation of law. Each certificate representing shares of capital stock of Old BIO-key outstanding immediately before the Reincorporation, is deemed from and after the Reincorporation for all corporate purposes to represent the same number of shares of capital stock of the Company.

As a result of the recent mergers, and as discussed in Note M to the Consolidated Financial Statements, we have organized BIO-key International, Inc. into three reporting segments: Law Enforcement, Fire Safety and Biometrics. During 2005, the Company continued to integrate the products, operations and technologies acquired from Public Safety Group, Inc. and Aether Systems, Inc.

## Products

BIO-key® operates in three major segments – biometrics, law enforcement and fire safety. These segments are described below and a list of products in each line is noted.

### *Biometrics*

BIO-key's finger identification algorithm – Vector Segment Technology (VST) is the core intellectual property behind its full suite of biometric products that include:

- **Vector Segment Technology SDK (VST)** – BIO-key's biometric development kit that provides developers the ability to take advantage of a highly accurate, device interoperable algorithm. VST is available as a low level SDK for incorporation into many complex application systems. VST runs in Windows, Linux or Solaris systems.
- **True User Identification®** – BIO-key's biometric identification solution that offers large scale one to many user lookup with nothing but a single fingerprint. This solution leverages the power of Oracle for large scale solutions in the millions of users, or uses smaller databases for more modest applications to 100,000 users.
- **WEB-key®** – BIO-key's biometric platform that offers an enhanced level of security by securing the user's authentication with trusted communications and simple use. WEB-key runs on Windows or Linux systems.
- **Biometric Service Provider** – BIO-key provides support for the BioAPI (a standards based solution meeting worldwide needs, see [www.bioapi.org](http://www.bioapi.org) for details) for a compliant interface to applications using biometrics for verification and identification. BIO-key enhances the traditional use of the BioAPI by adding support for CE devices, supporting identification calls and also providing a single user interface for multiple fingerprint readers.
- **ID Director** – BIO-key's solution for single sign on integration with Computer Associates SiteMinder, Oracle's Fusion Middleware SSO, and other solutions, utilizing the power and security of WEB-key. This solution provides a simple to implement, custom authentication scheme for companies looking to enhance authentication and add a level of security and audit through re-authentication of a user at the transaction level.

The Company's biometric identification technology improves both the accuracy and speed of finger-based biometrics. The Company's proprietary biometric technology scans a fingerprint and identifies a person, typically within a few seconds or less, in databases of a million people or more. BIO-key can accomplish this without using any other identifying data – a key differentiator for BIO-key since other biometric solutions may also require traditional token/card identification. BIO-key's core technology supports user enrollment on over 40 different commercially available readers and in turn can offer compatibility among those readers through a single fingerprint template. We have also added INCITS 378-2004 support to our software development kits which makes our products compatible with all of the Registered Traveler projects, PIV initiatives, and FIXS consortium solutions. We believe our fingerprint identification technology has a broad range of possible information security and access control applications, including:

- Securing Internet sites and electronic transactions
- Securing access to logical networks and applications
- Securing access to buildings and restricted areas
- Providing fast, accurate member identification services
- Securing mobile devices such as cell phones and PDA's
- Preventing identity theft with positive identification and false alias validation



*Law Enforcement*

- **MobileCop** A complete wireless query and messaging application that puts the power of mobile and wireless technology to work for agencies of every size, MobileCop sets the standard for mobile law enforcement. Providing real-time retrieval of motor vehicle, warrant and criminal history information, powerful mobile integration capabilities, and an intuitive user interface, MobileCop delivers the most in performance and it's easy to see why over 1,200 law enforcement agencies around the country have deployed MobileCop for fast and secure access to critical information in the field.
- **PocketCop®** PocketCop® is a software solution that provides police officers and other security personnel instantaneous access to important criminal, civil, and private database information in a wireless environment. PocketCop® is a handheld application that allows law enforcement officers to access state and federal databases over the wireless network for Palm OS, Windows CE, and Pocket PC. Using a portable wireless handheld device and the PocketCop® application software, an authorized user can access suspect information such as wanted status, warrant status, vehicle registration and driver license status. PocketCop® technology has been deployed in numerous police departments in the United States, including the deployment for the Massachusetts State Police.
- **IdentityMatch** - a web-based system that allows law enforcement agencies to capture and store fingerprints online and to identify subjects by matching their fingerprint against those stored in the database, securely and in real time. Fingerprints can be captured using a live scan device from existing 10-print cards or through a wide variety of inexpensive commercially available fingerprint readers. This is an AFIS companion, not a replacement, product designed to maximize the value of fingerprint data and also to provide a new level of safety for the law enforcement personnel.

BIO-key also provides a number of optional features designed to augment the core Law Enforcement products. These include:

- **Field Interview Tracker** - enables personnel to capture field contact information. The data is stored in a searchable database where it can be located quickly. Police agencies can create online contact forms that meet their specific needs and multiple agencies can share information while using their own forms and procedures.
- **TStop** - was developed to enable law enforcement agencies to comply with state mandated and voluntary traffic stop reporting. Law enforcement personnel can capture the required information on their mobile computer and transmit it to the server where it is stored and can generate reports.
- **State Crash Report** - enables personnel to use their mobile computer to collect data needed for their state's crash report. This data can be wirelessly transmitted to a server so a supervisor can review and approve it. Once complete the report can be printed in the state's format. Only selected states are supported.
- **Multiple Application Programming Interface (API)** - allows an agency to have multiple ports to the server to accommodate disparate interfaces. These multiple API ports are in addition to the one port that is inherent in the server as well as the State/NCIC interface.
- **Incident Command** - using FieldSoft's PDonScene, this solution is used by both patrol and tactical teams, such as a SWAT, to manage people and resources at the scene of an incident or at a central location such as an emergency operations center. It can also be used for general event management.
- **InfoServer** - BIO-key's solution for an agency's central messaging switch for application software service, State/NCIC interfaces, Computer Aided Dispatch (CAD) and Records Management Software (RMS) interfaces, data sharing and other applications.





### *Fire Safety*

In addition to law enforcement/fire service mobile data solutions, BIO-key offers its Sunpro fire service/EMS records management software, FireRMS , that helps large and small agencies manage operations, track incidents and support fire prevention initiatives. FireRMS Mobile provides wireless query and messaging solutions that extend computer aided dispatch, fire records, and other in-house data sources to a mobile environment and provide mission-critical information to emergency response personnel where and when they need it.

- **PacketCluster® Rescue** BIO-key s mobile information solution for fire and EMS, runs off the same server as MobileCop . It provides much of MobileCop functionality without the State/NCIC interface not required by fire service and EMS. Rescue provides mission-critical data such as HAZMAT information and building plans that fire service officers need to know while at a fire scene.
- **FireRMS Records Management Software** this NFIRS 5.0-compliant fire records system helps manage operations, track incidents and support fire prevention initiatives. It is designed to speed data entry and reduce completion time for front-line personnel.
- **CAD Interfaces** CAD interfaces provide a connection between BIO-key records and all major CAD systems with the most comprehensive real time integration. Incident reports are opened as soon as CAD dispatches a call. Incidents are current and ready to complete when the crew returns to the station, streamlining and improving the accuracy of incident reporting.
- **RMS Interfaces** RMS interfaces provide a mechanism to integrate patient care reports collected in the field with the NIBRS report. Patient data is populated in the appropriate fields, eliminating redundant data entry.
- **Other Interfaces** BIO-key provides interfaces to other third party solutions including EMS billing, EMS county/state interfaces, professional staffing solutions and others.

BIO-key also offers the following Fire/EMS Partner solutions:

- **EMS Field Data Collection** Regist\*r Express from MedDataSolutions enables EMS field data collection for efficient collection of patient data where it is generated.
- **Geographic Data Analysis** FireView from the Omega Group allows Fire and EMS agencies to analyze their deployment strategies.
- **Personnel Staffing** Telestaff from PDSI automates and manages complex Fire/RMS agency staffing needs and is integrated with FireRMS s Personnel and Roster modules.
- **Incident Command Module** FDonScene by FieldSoft provides incident management, responder accountability, and tactical survey or preplan browser software solutions. FDonScene interfaces with PacketCluster Rescue to support incident management-en route or on scene.

### **Current Business Plan**

BIO-key s current business plan is to:

- **License its core technology VST and True User Identification®** to original equipment manufacturers, systems integrators, and application developers who develop products and applications that utilize its biometric finger matching solutions.

- **License WEB-key®**, the Company's security centric web-based biometric authentication solution.
- **Provide for device independent finger identification matching** for virtually any application by using the latest advances in scanning technology.
- **License its wireless software solutions for the public safety market** directly to counties, cities and towns across North America as well as through systems integrators and resellers.
- **Leverage its FireRMS suite of products** for the growing Emergency Medical Service data collection and reporting market.
- **Integrate its core technology competencies** to leverage new business opportunities and develop new markets for its innovative products.

4

---

## Markets

### *Law Enforcement*

BIO-key's InfoServer, MobileCop and PocketCop® Law Enforcement products are the leading wireless mobile data communications client/server solution, implemented in more than 1,200 agencies nationwide. Providing immediate access to mission-critical data and enabling in-field reporting, BIO-key software keeps officers on the street, improving their productivity and enhances officer safety. BIO-key solutions are able to run across any and all wireless infrastructures and integrate with virtually all computer-aided dispatch (CAD) and records management systems. This makes us a proven leader in multi-agency cooperation and interoperability, which are absolutely critical in times of large-scale natural and terrorist threats.

- *Growth potential* BIO-key's large base of more than 1,200 law enforcement agencies continues to be a strength that helps leverage additional sales from both existing customers and new customers. A key opportunity is the growing awareness of the need for multi-agency interoperability. In these situations, BIO-key offers:
  - BIO-key's LE products can run on any and all wireless infrastructures. BIO-key also has proven success implementing seamless roaming across multiple infrastructures for multi-agency consortiums.
  - BIO-key's open architecture.
  - BIO-key has experience in large, complex and multi-agency implementations such as Hamilton County, Ohio, Sheriff's Office and Pennsylvania State Police.

These capabilities position BIO-key well to work with leading CAD vendors, even with vendors that have mobile data solutions but do not have the depth of interoperability capability that BIO-key offers.

An additional growth area is the introduction of BIO-key's finger-based biometric identification to law enforcement. In addition to now offering biometric login to our traditional InfoServer product, we have introduced the IdentityMatch fingerprint identification solution, which lets law enforcement personnel capture fingerprints in the field and, using BIO-key's patented Vector Segment Technology®, then analyzes and categorizes fingerprints the same way a fingerprint expert would only faster. IdentityMatch also enables multiple law enforcement agencies to share fingerprint data with other agencies. This powerful tool, built on BIO-key's understanding of law enforcement requirements and its fingerprint technology, present opportunities for the law enforcement business segment in the coming year.

### *Fire Safety*

BIO-key's FireRMS fire records management software is a flexible solution available for Fire Service and EMS agencies. It is a comprehensive collection of modules that manage a range of activities from daily scheduling to vehicle maintenance. FireRMS streamlines data collection across all areas of department operations, and integrates with other department systems to provide a seamless solution for data access, whether in the station or on the scene of an incident. In addition to helping first responders efficiently deliver traditional fire safety and services and respond to massive emergency situations, it enables adherence to NFIRS, NEMSIS, HIPAA, and ISO requirements. The solutions also bring the station into the field with mobile data communications solutions, and most recently, FireRMS Mobile, which brings the capabilities of FireRMS to first responders where and when they most need to report and access critical information.

- *Growth potential* a growth opportunity for the fire business segment is in the mobile market with the RMS mobile products. BIO-key's FireRMS Mobile solutions extend the power of our FireRMS product to the field. Inspectors, for example, can now perform occupancy inspections over a wireless or synched connection using a pen tablet. This approach eliminates redundant data entry, and provides immediate updates of critical information and notification of violations. Likewise, EMS workers can collect critical patient data and relay the data to medical personnel. This new mobile approach to fire and EMS data collection and access offers great potential among both new and existing

FireRMS customers.

*Finger-based Biometric Identification*

Finally, BIO-key is a leader in finger-based biometric identification. In partnerships with OEMs, integrators, and solution providers, we provide biometric software solutions to private and public sector customers. BIO-key's patented vector segment technology is the foundation for these solutions.

5

---

BIO-key's WEB-key® is a cost-effective, easy-to-deploy, fingerprint-based strong authentication system. This unique solution allows users to positively identify themselves to any application with the simple scan of their finger. This capability is a significant improvement in both convenience and security over other alternatives and provides companies with a cost-effective solution to thwart phishing attacks and comply with government regulations and legislation such as FFIEC compliance, HIPAA, Sarbanes-Oxley, and the Electronic Signatures Act. BIO-key couples these capabilities with device interoperability and system flexibility and scalability. BIO-key enables the use of about 40 different fingerprint sensor technologies to enroll and identify employees, customers or business partners. Most recently, BIO-key integrated its biometric capabilities with its public safety mission with the introduction of IdentityMatch™, a real-time, in-station solution that allows law enforcement professionals to capture fingerprints from a suspect or captured from a crime scene and compare them to fingerprints. BIO-key has also formed relationships with providers of biometric logon software like IdentiPHI, Softex, and Computer Associates to provide enterprise-ready SingleSignOn systems to many large companies in the US and abroad. Also, BIO-key has integrated to a pure physical access solution in NextGenID, which has been deployed at BIO-key facilities.

- *Growth potential* As the provider of the core technology, BIO-key's greatest growth potential for this market is as a partner with companies that offer cutting-edge applications that address growing concerns particularly about identity theft and terrorism.

For example, BIO-key has implemented programs that will enable biometric access. These include a national pilot with a large fitness center chain to provide finger-based membership and access to its locations around the country; with IdentiPHI to provide strong network based authentication on BIO-key technology; and with the Pegasus Program to authenticate users accessing a nationwide information-sharing system designed by and for the nation's sheriffs. These represent the kind of partnership-based opportunities BIO-key may see in the finger-based biometric market.

In parallel, BIO-key is both strengthening security and improving user and system administrator convenience by integrating biometric log-in, as well as two-factor authentication, with its law enforcement and fire safety products. This is a true differentiator to potential new customers, and creates add-on opportunities with existing customers.

## **Competition**

The markets for BIO-key products and technologies are developing and are characterized by intense competition and rapid technological change. No assurance can be given that our competitors will not develop new or enhanced technologies that will offer superior price, performance, or features, or render BIO-key products or technologies obsolete.

### *Biometrics*

In addition to companies that provide existing commonplace methods of restricting access to facilities and logical access points such as pass cards, PIN numbers, passwords, locks and keys, there are numerous companies involved in the development, manufacturing and marketing of fingerprint biometrics products to commercial, government, law enforcement and prison markets. These companies include, but are not limited to, Cogent, NEC, IDENTIX, Sagem-Morpho, and Bioscrypt.

The most recent automated fingerprint identification product sales in the market have been deployed for government and law enforcement applications, typically at more cost than BIO-key's products and licensing arrangements. Although most companies that target consumer application markets have completed development of their biometric products, such technologies have not been widely accepted in the commercial markets to date. Most companies competing for commercial opportunities are in the business of selling scanning devices and tie their algorithm to a specific device. BIO-key has created a device independent algorithm that provides flexibility in choosing the correct device and optical or tactile sense to fit the application served.

BIO-key has found that commercial markets have been slow to widely purchase biometrics as a viable alternative to their current security methods. As a result, the primary competition for biometric technology consists of traditional security methods such as passwords, PINs, cards, and tokens.

With respect to competing biometrics technologies, each has its strength and weaknesses and none has emerged as a market leader:

- *Fingerprint identification* is generally viewed as inexpensive and non-intrusive.
- *Iris scanning* is viewed as accurate, but can be expensive and inconvenient to use.

- *Facial recognition* has recently received substantial attention; however, it can have accuracy limitations and be highly dependent on ambient lighting conditions, angle of view and other factors.

The market for biometric technology is evolving. Computer breaches, identity theft, phishing and other events in the recent past are driving a large-scale shift to biometric deployments. In addition, companies such as IBM, Dell, Gateway, MPC, Samsung and HP have all introduced computers with integrated finger scanning devices to complement the conventional username/password technique since it is highly susceptible to hackers and security breaches. BIO-key supports these integrated devices for broader enterprise level security solutions.

6

---

*Law Enforcement*



## Edgar Filing: BIO KEY INTERNATIONAL INC - Form 10KSB/A

The public safety market comprises agencies at all government levels, with a range of users, from a few to many hundreds. BIO-key competitors in the mobile data market include Computer Aided Dispatch/Records Management companies such as Printrak, InfoCop and Motorola. Each has comprehensive CAD and/or RMS offerings and has augmented those with their own mobile data and field reporting solutions. While these solutions may not be as functionally rich as the BIO-key suite of products, they are sometimes less expensive. They also provide a complete solution from one vendor.

### *Fire Safety*

The fire records management market includes a large number of RMS vendors including Firehouse, FDM and ETI. These and other competing companies represent a wide range of organizations, from large integration companies, to small garage companies, and offer products similar in scope to BIO-key's FireRMS. The functionality and price of these products also encompass wide ranges of features and costs.

### **Marketing and Distribution**

BIO-key's marketing and distribution efforts comprise the following major initiatives:

- During the past year, BIO-key has strengthened its alliance with Oracle and has been recognized as a Certified Partner in the Oracle Partner Network. BIO-key supports the Oracle e-business suite of applications and provides the biometric enabler for the Oracle Single Sign on product. As an Oracle development partner, BIO-key provides the underlying database used for true user identification and on demand alias checking. As a development partner, BIO-key participates in Oracle Trade Shows such as Oracle Open World and Oracle Apps World.
- BIO-key has strategic alliances with technology leaders including Oracle, Netegrity, Hewlett Packard, Dell, Verizon, Sprint/Nextel, Cingular and others.
- BIO-key is also promoting biometric technology and its offerings through industry trade shows, public speaking engagements, press activities and partner marketing programs
- BIO-key is directing licensing efforts to original equipment manufacturers, application developers and system integrators.
- BIO-key is building a reseller, integrator and partner network as well as a direct sales team.

Following are the specific marketing/sales programs in place:

- *Direct Selling Efforts* BIO-key now has a base of area sales directors who are responsible for both the law enforcement and fire safety markets. This team of sales professionals brings extensive experience in technical solution and relationship-based selling. They are supported by a pre-sales team that includes system engineering and proposal management and a post-sales program management, implementation and training professionals. Included in this team are individuals who are themselves former police officers and firefighters.

BIO-key's direct sales force also includes area sales directors for the OEM and Federal Government markets, each of whom brings not only extensive sales experience but also expertise in emerging biometric technologies. The BIO-key sales force is rounded out by Inside Sales, which is responsible for maintaining and supporting our existing install base, acting as a front-line support for any inquiries on our product line, and facilitating activities that make the field team more productive.

- *Conferences and Trade Shows* BIO-key attends and actively participates in various product-related conferences and trade shows in the technology and security industries to generate market awareness of biometric and wireless mobile data technology generally and our offerings specifically. BIO-key's public safety software often is featured at our business partners' booths at these events, showcasing the interoperability of the two products.
- *Strategic Alliance* BIO-key's strategic alliances and reseller agreements with other vendors play a significant role in our overall sales efforts. In the past year, BIO-key has initiated and bolstered numerous important and promising long-term relationships. Just a few examples include:

### Law Enforcement

- BIO-key is partnering with Cingular, the largest wireless carrier in the country, to first responders in a seven-county Tennessee consortium of fire, police and EMS agencies in access to mission critical information using MobileCOP solution in conjunction with Cingular's nationwide\* EDGE wireless data network
- The Omega Group continues to provide FireView software mapping tools that help review existing deployment policies and develop new strategies, to complement BIO-key's range of solutions for Fire/EMS agencies.
- BIO-key now resells solutions from ThreatScreen that provide an exposure-diagnostic/identification, data collection, and reporting tool to first responders so they can quickly assess victims to determine chemical, biological, or nuclear agent exposure.

7

---

- Silex Technology America, Inc., which develops fingerprint reader products designed to support a variety of secure computing options, utilizes BIO-key's VST and WEB-key technology.
- *Strategic Marketing Alliance* BIO-key has established a strategic marketing alliance with Hewlett Packard to provide BIO-key handheld technology for the Massachusetts State Police.
- *Reseller Relationships* BIO-key has established reseller relationships with companies that resell BIO-key public safety software.

### Licensing

BIO-key targets both Internet infrastructure companies and large portal providers as possible licensees for its WEB-key® solution. On the Internet infrastructure side, BIO-key seeks to partner with Internet server manufacturers, providers of database and data warehouse engine software, horizontally positioned application engines, firewall solution providers and peripheral equipment manufacturers. On the portal side, BIO-key is targeting financial service providers such as credit and debit card authorization and issuing institutions, Internet retailers, business-to-business application service providers (ASPs) and corporate intranets. In the past three years, BIO-key has undertaken a WEB-key® and VST direct selling effort, and entered into license agreements with OEMs and system integrators to develop applications for distribution to their respective customers.

BIO-key is also addressing the security needs of application providers in the following vertical markets:

- *Government* Using BIO-key's technology, Northrup Grumman deployed an application within the Department of Defense to cross-credential visitors and contractors to certain military bases.
- *Education* Educational Biometric Technologies, Lunch Byte Systems and Identimetrics have incorporated BIO-key technology to enable school children to pay for school lunch programs and checkout library books using their fingerprints. VST technology enables schools to enroll these children and reduces the administrative costs of managing passwords and collecting payments.
- *Commerce:* ChoicePoint has implemented a check cashing solution using BIO-key's VST technology to reduce fraud and identity theft.
- *Patient Records and Information Management:* HBOC, one of the largest healthcare patient records and information management companies, has integrated BIO-key technology into their portal and has deployed their solution in a pilot for the Baptist Hospital System.
- *Financial:* BIO-key is working with several companies focusing on financial applications such as point of sale systems and employee trusted identification cards, as well as customer facing applications over the Internet. BIO-key has also begun work with several financial institutions to incorporate its technology for secure access to money transfers for institutional customers.

### Intellectual Property Rights

We believe that our intellectual property is important to our biometric, law enforcement and fire information management segments:

Patents our biometrics segment uses patented technology and trade secrets developed or acquired by us. In May 2005, the U.S. Patent Office issued us a patent for our Vector Segment fingerprint technology (VST), BIO-key's core biometric analysis and identification technology. Additionally, we have a number of U.S. and foreign patent applications in process related to this intellectual property.

## Edgar Filing: BIO KEY INTERNATIONAL INC - Form 10KSB/A

**Trademarks** We have registered our trademarks ( BIO-key , SACman , SACcat , SACremote , True User Identification , WEB-key , PacketCluster Patrol , PacketWriter , PacketBlue , SunPro and the design mark for Ceurulean with the U.S. Patent and Trademark Office. We also applied for trademarks for PocketCop and Cerulean .

**Copyrights and trade secrets** We take measures to ensure copyright and license protection for our software releases prior to distribution. When possible, the software is licensed in an attempt to ensure that only licensed and activated software functions to its full potential. We also take measures to protect the confidentiality of our trade secrets.

### **Research and Development**

Our research and development efforts are concentrated on enhancing the functionality, reliability and integration of our current products as well as developing new and innovative products for the biometrics, law enforcement and fire markets. Although BIO-key believes that its identification technology is one of the most advanced and discriminating fingerprint technologies available today, the markets in which BIO-key compete are characterized by rapid technological change and evolving standards. In order to maintain its position in the market, BIO-key will continue to upgrade and refine its existing technologies.

8

---

In 2005, BIO-key announced the launch of IdentityMatch, our fingerprint identification system. IdentityMatch offers a tool for agencies to store and search fingerprints and the associated demographic data, the ability to compare new prints with those previously captured as a low-cost AFIS alternative or to be used for a wide variety of routine identification transactions not supported by AFIS. IdentityMatch is currently being tested by a number of customers.

During fiscal years ended December 31, 2004 and 2005, BIO-key spent approximately \$2,980,000 and \$6,846,000 respectively, on research and development. BIO-key's limited customer base during that time did not directly bear these costs, which were principally funded through outside sources of equity and debt financing.

#### **Government Regulations**

BIO-key is not currently subject to direct regulation by any government agency, other than regulations generally applicable to businesses or related to specific project requirements. In the event of any international sales, the company would be subject to various domestic and foreign laws regulating such exports and export activities.

#### **Environmental Regulations**

As of the date of this report, BIO-key has not incurred any material expenses relating to our compliance with federal, state, or local environmental laws and does not expect to incur any material expenses in the foreseeable future.

#### **Employees and Consultants**

BIO-key currently employs one-hundred (100) individuals on a full-time basis: fifty-one (51) in engineering, customer support, research and development; Thirteen (13) in finance and administration; and twenty-six (26) in sales and marketing. BIO-key also uses the services of ten (10) consultants who provide engineering and technical services.

### **RISK FACTORS**