Feltl and Company

SECURITIES BROKERAGE AND INVESTMENT BANKING

Feltl and Company Research Department
225 South Sixth Street, Suite 4200
Minneapolis, MN 55402
1.866.655.3431

Jay M. Meier
jmmeier@feltl.com | 612.492.8847

Vasco Data Security

Identity Management *June 9, 2010*

Company Description: Vasco Data Security is a leading provider of One-Time-Passcode credentialing systems used by banking institutions and large enterprise to secure and protect access to high value assets and environments.

Initiating coverage of Vasco Data Security with a HOLD rating and $5.50 target

(VDSI - $5.83) HOLD

Key Points

- VDSI is a leading One-Time-Passcode (OTP) provider for access control and e-commerce.
- We believe the OTP model is flawed and will be marginalized by modern identity management standards requiring PKI and biometrically enabled smartcards.
- VDSI's business is concentrated in European banking. The European sovereign debt, banking and economic crisis creates risk. FOREX may also provide significant near-term headwinds.
- Solid balance sheet and a fair valuation limit downside, but we rate VDSI a HOLD with a $5.50 target.

Financial Summary

Rev(mil)	2009A	2010E	2011E
Mar	$23.2	$23.9A	
Jun	$24.5	$27.3E	
Sep	$22.1	$26.1E	
Dec	$31.9	$35.5E	
FY	$101.7A	$112.7E	$129.5E
P/Sales	2.2x	2.0x	1.7x

EPS	2009A	2010E	2011E
Mar	$0.09	$0.01A	
Jun	$0.05	$0.03E	
Sep	$0.04	$0.04E	
Dec	$0.15	$0.07E	
FY	$0.33A	$0.16E	$0.20E
P/E	17.7x	36.4x	29.2x

Price:	$5.83
52-Week Range:	$8.98 -$5.82
Target:	$5.50
Rating:	HOLD
Shares Outstanding:	38.3 mil
Mkt. Capitalization:	$223 mil
Ave. Volume:	110,000
Instit. Ownership:	10%
BV / Share:	$2.76
Debt / Tot. Cap.:	0%
Est. LT EPS Growth:	14%

Vasco Data Security is a leading provider of One-Time-Passcode authentication systems and may emerge in smart card credentialing, device management and authentication systems. Vasco Data Security supplies software, hardware and systems that secure and control access to both physical and logical environments. Vasco is a leading provider of One-Time-Passcode and potentially other device authentication systems. Its core products are software platforms that connect and manage handheld credentials to a user's identity and those people's privileges, primarily in network access control and e-commerce.

The global OTP market may approach $700mm in 2015, but the OTP model may be flawed and could be displaced by smartcard credentialing solutions. Frost & Sullivan estimates the One-Time-Passcode (OTP) market will grow to $690mm in 2015 from $430mm in 2008, a 7.7% CAGR. While OTP has attained some growth in recent years, emerging credentialing and identity management standards require PKI and biometrically enabled smart card credentials that could marginalize OTP. Further, we believe the OTP model may be flawed. OTP vendors, including Vasco may be forced to diversify away from OTP, toward smartcard credentials, PKI and biometrics.

Vasco's concentration in European banking poses a near term risk. The vast majority of Vasco's sales has come from the Europe-Mid East-Asia (EMEA) region and has been concentrated in banking. The current uncertainty surrounding EU banking, the EU economy and sovereign debt may create headwinds for the Company. The abrupt reversal of the Euro vs. the U.S. dollar during the quarter, may create additional risk.

Initiating coverage of VDSI with a HOLD rating and a $5.50 price target. VDSI may present a fair valuation profile, but it must demonstrate a meaningful migration toward smartcard credentialing and faces potentially significant economic headwinds that may hamper results.

Investment Thesis:

Terrorism, identity theft and fraud are pervasive, costing society billions annually. International and domestic governments have re-examined global credentialing, privileging, and access control systems and released standards that are visible today, standards now required by both international and domestic (U.S.) law enforcement agencies for implementation in critical infrastructure industries. Therefore, we believe demand for advanced authentication and identity management systems will grow relatively rapidly over the coming years. Vasco Data Security is a leading provider of OTP and other credentialing management systems and may be well positioned to participate. However, we believe the OTP model is fundamentally flawed and competing technologies, namely PKI and biometrically enabled smartcard credentials, are likely to displace OTP solutions over time. Thus, VDSI may experience headwinds until it successfully diversifies its product offering.

Please see important disclosures on pages 12-14.

Initiating Coverage of Vasco Data Security (VDSI) with a HOLD rating

Company Description and History:

Vasco Data Security supplies software, hardware and systems that secure and control access to both physical and logical environments. Vasco is a leading provider of One-Time-Passcode (OTP) credentialing systems, device management systems and device authentication systems, including limited Public Key Infrastructure (PKI). The Company's core products are software platforms and systems that connect and manage handheld credentials to a user's identity and that persons entitled privileges. These platforms are commonly used to control access to logical domains, like computer networks, web-based infrastructures, portals, services and virtual private networks. The backbone of Vasco's product suite is the VACMAN Controller, a middleware server platform supporting multiple authentication technologies, including passwords, OTP tokens, electronic signatures, digital signatures, PKI certificates and biometrics. The VACMAN Controller interfaces with a DIGIPASS device, issued to and operated by the end-user/consumer. Vasco offers customers a large variety of user authentication modalities, including passwords, OTP and smartcards. However, the vast majority of Vasco's revenues to date are from OTP. Vasco launched its "DIGIPASS as a Service" business model in early 2010, providing customers the ability to mix and match best suited authentication modalities. The end-user credential may thus become less important to Vasco's business than their ability to validate a credential and, potentially more importantly, accommodate evolving authentication standards.

The Company was founded as VASCO Corp. and entered the data security market in 1991 through the acquisition of Thumbscan, Inc. In 1996, VASCO Corp. acquired Lintel Security NV/SA, a developmental Belgian corporation focused on OTP security tokens. Further, VASCO acquired Digipass NV/SA, another Belgian token developer in 1996. The Company was renamed Vasco Data Security NV/SA in 1997. Vasco has since completed seven additional tuck-in acquisitions, including assets involving smartcards, digital signatures and basic public key infrastructure (PKI). Vasco opened its international headquarters in Zurich, Switzerland in 2006, established a presence in Brazil and Japan in 2007, and subsequently entered India. The Company has several patents regarding its capabilities, primarily covering the DIGIPASS product line, but limited IP creating significant barriers to entry to the market. Its patents expire between 2010 and 2022. Vasco employs roughly 294 people, with 27 in the U.S., 222 in EMEA, 15 in APAC and 30 in other countries. Vasco's US headquarters are located in Oakbrook Terrace, Illinois. Its international headquarters are located in Zurich, Switzerland. Its European operating headquarters are located in Wemmel, Belgium. The website is www.vasco.com. The Company's fiscal year ends in December.

Vasco has over 9,500 customers (including over 1,400 banks), in over 100 countries. Banking, including retail-oriented online banking and e-commerce, remains the Company's primary sales vertical, but enterprise-security customers represent a large part of Vasco's new customers over the last three years. High-end video and online gaming have also emerged as potential growth markets. The Company sells its products both directly and through an established channel of 71 system integrators, Value Added Resellers (VARs) and distributors. Bell Micro and Tech Data are key distributors for the Company. Samsung Semiconductor is Vasco's primary supplier of token microprocessors. Vasco's top ten customers represented 34% of sales in FY'09. Roughly 93% of Vasco's sales and 83% of expenses were incurred outside the United States, primarily in Europe. The Company markets its products based on several themes, including speed and ease of implementation/administration, reliability, interoperability with existing applications, scalability and overall cost of ownership. Its platforms are designed for flexibility and accommodate the most diverse network environments. Vasco markets its platform as a "full option, end-to-end authentication" offering and can accommodate a wide range of security and budget needs.

Investment Thesis:

The 9/11 tragedies exemplified risks with insufficient credentialing and access control. Identity theft and fraud are also pervasive, costing society billions annually. International and domestic governments have re-examined global credentialing, privileging, and access control systems and released standards that are visible today. Those standards are now required by both international and domestic (U.S.) law enforcement agencies for implementation in critical infrastructure industries. Therefore, we believe demand for advanced authentication and identity management systems will grow relatively rapidly over the coming years. Vasco Data Security is a leading provider of OTP and other credentialing management systems and may be well positioned to participate. However, we believe the OTP model is fundamentally flawed and competing technologies, namely PKI and biometrically enabled smartcard credentials, are likely to displace OTP solutions over time. Thus, the Company may experience headwinds until it successfully diversifies its product offering.

Management:

T. Kendall "Ken" Hunt is Vasco's founder, Chairman of the Board and CEO. While he has served as Chairman since the Company's incorporation, he served as CEO from 1997 through 1999 and returned to be CEO again starting in 2002. He is affiliated with several high-tech start-ups and has served as a Director of Global Med Technologies. He has served as an Advisor to many business and technology associations. He holds an MBA from Pepperdine University and a BBA from the University of Miami. He is 66 years old.

Jan Valcke serves as President and COO, positions he has held since 2002, and he has been an officer of the Company since 1996. Prior to Vasco, he was VP of Sale/Marketing at DigiPass NV/SA. He co-founded The Digiline Group in 1988. He holds a degree in Science from St. Amands College in Kortrijk, Belgium. He resides and works in Belgium.

Clifford K. Bown has served as Vasco's Exec.-VP and Chief Financial Officer since 2002. He began his career with KPMG, LLP and has directed audits of many publicly held companies. From 1991 to 1993, he acted as CFO for XL/DataComp, a midrange technology and support company. Mr. Bown also worked as CFO at companies in the insurance and healthcare industries. He received a B.S. in Accountancy from the University of Illinois, Urbana and an MBA from the University of Chicago. He also has a CPA certificate.

Primary Markets, Solutions and Products:

Vasco sells its products to customers interested in controlling or securing access to privileges and things. Central to access control is the privilege holder's identity. Thus, VSDI's products facilitate connecting a privilege with a user or applicant identity. Historically, we have connected privileges with identities by issuing a credential that associates the privilege with the owner of the credential. Driver's licenses, travel documents, employment ID, student ID, credit cards and other credentials all associate a user/holder with a granted privilege. Vasco products enable privilege grantors to better manage the issuance and control of the privilege credential and its rightful owner. Three primary market verticals for such relationships include Employer-to-Employee (E2E), Business-to-Customer (B2C) and Government-to-Citizen (G2C). Each market vertical is somewhat unique, requiring varying levels of security assurance. However, the expense of the credentialing system tends to rise with the sophistication of the system. Thus, the level of system sophistication and expense tends to parallel security requirements and certain types of privilege issuers tend to gravitate toward more or less sophisticated platforms, depending on their perception of risk. Thus, the Company's core product-sets for each vertical are similar, but vary in breadth and robustness depending on customer requirements. At the core, these solutions utilize some level and combination of strong authentication products and credential management to mitigate varying levels of risk associated with regulatory and policy compliance, asset loss, theft and vandalism. Core products include:

VACMAN: The VACMAN Controller is Vasco's core authentication platform. VACMAN integrates into virtually any network and accommodates all of Vasco's credentialing offers, including One-Time-Passcodes (OTP), passwords, biometrics, PKI and other data. The VACMAN controller is the backbone of Vasco's security system and interfaces with issued credentials and identities in the fields. It enables policy administration and basic lifecycle management. Fully enabled with various VACMAN Middleware packages, the VACMAN Controller functions as the back-office enterprise access control. Once enrolled in the VACMAN system, each end-user/consumer can utilize the issued credential, typically a DIGIPASS token, to help authenticate the user during an access control negotiation.

IDENTIKEY: IDENTIKEY is a fully functional authentication server and adds e-signature capabilities to the core VACMAN Controller. IDENTIKEY is designed to add secondary layers of security, primarily e-signature, to the OTP platform. It's been developed particularly for e-gaming, online gaming, e-banking and Virtual Private Networks (VPN).

aXs Guard: There are two aXs Guard appliances, the Identifier and the Gatekeeper. The Identifier is a standalone authentication solution offering 2-factor authentication specifically for remote access to a corporate network or web-based business applications. The Gatekeeper is actually a portfolio of potential security measures, including both DIGIPASS capabilities with traditional intrusion detection and antivirus, along with reporting and monitoring.

DIGIPASS: DIGIPASS's are the tokens and calculate dynamic passwords and signatures. A sophisticated algorithm incorporates enrollee-specific data, like a birth date and street address number for example, and time/date specific data to produce a defined series of numeric values that are specific to the consumer-enrollee at that point in time. Given any point in time, the algorithm will produce a small series of specific numbers. Because of their time-specificity, the values are described as "one-time" in nature. Hence, "one-time-passcodes" that are unique to the enrollee in the system, that identity that is associated with a given privilege entitlement, at a given time. The same algorithm, along with identity enrollee data, resides in both the VACMAN controller and the DIGIPASS. Thus, the two devices and only those two devices will generate the same set of OTP values per given time. Upon access control query, the token holder is prompted to generate and enter the OTP for confirmation of a match with the values produced by the server. Access is denied unless the user enters a matched OTP. Vasco offers 50 different varieties of OTP generating tokens that may be more suitable for a specific application. The OTP generator can be downloaded to a smart or cell phone, a PC, or browser. OTPs can be delivered via SMS messaging or via automated phone attendant if the end-user does not have the valid token in hand, but can produce personal identification data like a PIN.

The Total Addressable Market is large, but fragmented and developing slowly.

The OTP, Credentialing, Device Management and Device Authentication markets are not easily measured. Addressable market definition is at issue and researchers tend to either aggregate markets or slice/dice them, depending on their perspective. Consequently, market estimates vary greatly. For example, Frost & Sullivan forecasts the “Smart Card Management Systems” market will grow from $72mm in 2005 to $218mm in 2015, a 12.4% CAGR. Conversely, IDC estimates the “Mobile Device Management Enterprise” market will from $260mm in 2008 to $405mm in 2013, a 9.2% CAGR. Frost & Sullivan further estimates the One-Time-Passcode (OTP) market will grow to $690mm in 2015 from $430mm in 2008, a 7.7% CAGR. Lastly, Frost & Sullivan estimates the Smart Card Market will grow from $5 billion (4.7bil units) in 2008 to $8 billion (7.3bil units) in 2015, a 6.6% CAGR. In our opinion, the lines between these markets are blurred and we question how to truly discern between these markets and other related markets like Public Key Infrastructure (PKI) and biometrics. Moreover, such estimates fail to describe nuances that materially impact the viability of one technology over another within a particular niche market. Thus, we don’t consider many of these estimates particularly indicative. For perspective, we consider that President Obama’s Cyber Security Review calls for the application of Federal Information Processing Standard #201 (PIV) to critical infrastructure industries, including but not limited to banking, healthcare, transportation and energy.

Number of Firms, Number of Establishments, Employment, and Annual Payroll by Employment Size of the Enterprise for the United States, Sectors (large employment size groups) - 2005

SOURCE: 2005 County Business Patterns. For information on confidentiality protection, sampling error, nonsampling error, and definitions, see http://www.census.gov/epcd/susb/introusb.htm and http://www.census.gov/csd/susb/defterm.html.

NAICS Sector	Enterprise Size	Firms	Establishments	Employment	Payroll ($1,000)
All Sectors (including those not listed)	**Total**	**5,983,546**	**7,499,702**	**116,317,003**	**4,482,722,481**
	<500 employees	5,966,069	6,420,532	58,644,585	2,012,581,741
	>500 employees	17,477	1,079,170	57,672,418	2,470,140,740
Utilities	**Total**	**6,660**	**17,326**	**633,106**	**46,292,766**
	<500 employees	6,459	7,937	109,175	5,764,524
	>500 employees	201	9,389	523,931	40,528,242
Manufacturing	**Total**	**288,568**	**333,460**	**13,667,337**	**600,696,305**
	<500 employees	284,536	298,286	6,038,792	227,207,868
	>500 employees	4,032	35,174	7,628,545	373,488,437
Transportation and Warehousing	**Total**	**169,086**	**211,150**	**4,168,016**	**154,375,938**
	<500 employees	166,946	176,625	1,586,501	52,421,618
	>500 employees	2,140	34,525	2,581,515	101,954,320
Information	**Total**	**75,261**	**141,290**	**3,402,599**	**203,129,725**
	<500 employees	74,147	80,837	890,289	46,565,598
	>500 employees	1,114	60,453	2,512,310	156,564,127
Finance and Insurance	**Total**	**259,983**	**476,806**	**6,431,837**	**446,739,512**
	<500 employees	258,310	307,021	2,128,868	124,287,962
	>500 employees	1,673	169,785	4,302,969	322,451,550
Admin, Support, Waste Mngt, and Remediation	**Total**	**320,252**	**369,507**	**9,280,282**	**255,399,069**
	<500 employees	316,766	327,089	3,619,717	101,086,459
	>500 employees	3,486	42,418	5,660,565	154,312,610
Educational Services	**Total**	**72,410**	**80,486**	**2,879,374**	**82,522,976**
	<500 employees	71,293	75,074	1,294,428	33,014,630
	>500 employees	1,117	5,412	1,584,946	49,508,346
Healthcare and Social Assistance	**Total**	**599,392**	**746,600**	**16,025,147**	**589,654,273**
	<500 employees	595,641	668,593	7,748,761	269,349,560
	>500 employees	3,751	78,007	8,276,386	320,304,713
Accommodation and Food Services	**Total**	**462,983**	**603,435**	**11,025,909**	**156,041,233**
	<500 employees	461,168	500,969	6,611,592	84,859,803
	>500 employees	1,815	102,466	4,414,317	71,181,430
Total Critical Infrastructure Industries, excluding Govt.	**Total**	**2,254,595**	**2,980,060**	**67,513,607**	**2,534,851,797**
	<500 employees	2,235,266	2,442,431	30,028,123	944,558,022
	>500 employees	19,329	537,629	37,485,484	1,590,293,775

According to the U.S. Economic Census, in 2005 there were roughly 6.0 million firms and 7.5mm business establishments in North America, defining an "establishment" as a facility location where paid employees conduct their responsibilities. Further, there were approximately 2.26 million firms within critical infrastructure industries like energy, transportation, healthcare, and financial. The listing does not include any level of government. According to the survey, there were 2.24mm firms with fewer than 500 employees and 19,329 firms with greater than 500 employees in the critical infrastructure space in 2005. Since civil ID background checks are now mandatory in most U.S. critical infrastructure industries, we assume each "critical infrastructure firm" is a strong candidate to invest minimally in identity management and credentialing. The ASP of a "smart card management system" will fall from $22,500 in 2005 to $20,199 in 2015, according to Frost & Sullivan. Assuming all firms with 500 employees or more (19329 firms) purchased a single smart card management system at $20,199 implies an U.S. market opportunity of $390 million. Further, we assume the remaining 2.24 million critical infrastructure firms, those with fewer than 500 employees, are more likely to deploy an appliance based system, which we speculate might cost $5000 per unit. Assuming each smaller firm deployed one unit suggests an addressable market of $1.12 billion in the U.S. alone. Thus, the Total Addressable Market for smart card management systems in the United States could exceed $1.4 billion.

Defining market participants and share is equally difficult. Identity management and credentialing is a highly fragmented industry and we view Vasco as a leader in OTP but not the management of smart credentials, identities, card issuance and life-cycles. However, the business case and value proposition of advanced credentialing management platforms is not yet appealing in low security environments simply because the value implied in knowing who is coming and going is not always high. Customer loyalty programs, for example, may not need sophisticated identity management systems, while employee credentialing at the Federal Reserve might. To this end, for example, Gartner sees as many as 26 distinct vendors within the 'Versatile Authentication Server and Service" industry. Additionally, many vendors supplying various components of the modern credentialing platform offer their own rudimentary credentialing management system that could compete, but typically today do not add much value. Thus, while there are many vendors superficially competing with Vasco, few actually do. We believe that highly sophisticated credentialing solutions, like those currently deploying in government and high-security infrastructures, will ultimately displace less sophisticated systems. Moreover, we believe that many currently visible user authentication methods, like OTP, are actually logically flawed and will eventually become obsolete and replaced by smart card based platforms. To follow, competing vendors focused on those technologies may not remain competitively viable in credential management. Thus, we believe Vasco's positioning as a technology and "mind-share" leader in the OTP space suggests it's more likely to struggle and lose share as the smart card credentialing market matures.

Problems with One-Time-Passcode authentication models

We question the viability of One-Time-Passcode platforms (OTP) over the long-term for three distinct reasons. First, in our opinion, OTP is a system that relies on false logic, implying that the presentation of an OTP reasonably assures that the legitimately entitled privilege holder actually executed the command to generate the password. In other words, modern OTP platforms rely on the presumption that the person pressing the token button is the rightful owner of the OTP token. Since it cannot always be reasonably assured that the legitimate OTP was generated by the legitimate owner of the token, the OTP itself is little more secure than a standard password/PIN platform. In fact, most OTP platforms provide the option to include a password/PIN system in combination with the OTP to help verify the holder of the token. This is often described as "two factors" or even "strong authentication", requiring both something held by the authorized person and something known by that person. Thus, without the password/PIN, the presentation of an OTP really only ensures that a valid OTP generator was present at the time of the transaction. The password/PIN authenticates the user; the token does not.

Second, distinct OTP systems typically don't interoperate or cross-authenticate competing tokens. Thus, services seeking stronger authentication using tokens must ask customers to use a specific vendor's token. Unless that token is registered in competing OTP platforms, consumers may need multiple tokens to authenticate themselves for various distinct services. This is a major hassle factor that has caused OTP vendors to cross certify their systems. This cross certification effectively renders all OTP platforms equivalent, leaving price the only competitive advantage. Thus, it's not surprising that OTP platform vendors like Verisign, RSA (EMC), ActivIdentity, SafeNet, Aladdin and Vasco now offer the opportunity to download a free OTP generator to the desktop or smart phone, in lieu of the token. This lowers cost. Yet, deployed this way, the OTP generator actually only serves as another form or layer of device authentication, which is exactly what digital certificates and Public Key Infrastructure does. Since most PCs, laptops, cell and smart phones are issued fully enabled with some type of PKI certificates to authenticate the devices before they are allowed to access a network, there really isn't any reason to use an OTP embedded in the device along side the certificate. Further, PKI vendors today have started selling their Certificate Authority validation capabilities as a subscription service, dramatically lowering the up front cost of deploying PKI.

Lastly, since 9/11, standards development groups for the identity management and credentialing industries have focused on PKI and biometrically enabled smartcard systems. Those standards and specifications don't require OTP. Thus, we aren't surprised to find rapid price compression and slowing growth rates in OTP. In our opinion, OTP is ultimately destined for the museum. We predict that PKI enabled contactless smart card credentials, in various form factors, will become pervasive along with biometrics. Various form factors will include smart card IDs, like driver's licenses and credit cards, as well as SIM card enabled smart phones. It is the biometric that ultimately will authenticate the rightful owner of the credential. Thus, the device is authenticated by PKI and the user is authenticated by the biometric.

Initiating Coverage of Vasco Data Security (VDSI) with a HOLD rating

Recent Results:

Vasco reported Q1'10 results broadly missed expectations. Net sales of $23.9mm grew 3% y/y, but missed the $27.4mm consensus estimate. Management suggested banking customers delayed budget spending for new projects and existing customers slowed existing projects. Further, management believes Vasco recognized some sales ahead of schedule, during Q4'09, drawing down Q1'10 orders. The Company opened 438 new account in Q1'10, including 52 banks and 386 enterprise customers. 74% of sales came from banking and 26% came from enterprise. 68% of sales came from Europe, 9% from the U.S., 5% from Asia and 18% elsewhere. The weak U.S. dollar benefited Q1 sales by roughly 4% over Q1'09. Gross margin of 70% fell y/y from 72%, despite sales shifting toward potentially higher margin enterprise business. Gross margin also benefited from favorable FOREX. Operating expense of roughly $16.0mm increased $4.0mm (33%) y/y, despite effectively flat sales. OpEx grew largely because of a benefit from the reversal of $1.7mm of long-term accruals associated with performance compensation that was unlikely to be realized. Further, Q1'10 OpEx was negatively impacted by $826k from FOREX. With net interest income of $131k and taxes of $282k, Vasco reported Q1'10 net income of $573k. GAAP EPS of $0.01 fell from $0.09 in Q1'09 and missed the $0.06 consensus estimate. Vasco generated roughly $1.5mm in Q1 EBITDA and roughly $8.5mm in operating cash flow. Operating cash flow was driven largely by a $7.1mm reduction of receivables. Vasco's balance sheet is quite strong and healthy. The Company closed Q1 with $76mm in cash, or $1.99 per share and no debt. DSOs were 83 days. DPOs were 16 days and inventory turns were 2.7x, in line with recent results.

Guidance and our Outlook

Vasco provides relatively basic guidance, typically consisting of estimated top-line growth rates and operating margin estimates. Entering FY'10, management guided FY'10 sales to grow by 15%-20% from FY'09. This suggests a FY'10 sales guidance range of roughly $117mm-$122mm. Further, Vasco suggested FY'10 operating margin would be 5%-10%. After reporting Q1'10 sales that were flat y/y, management reiterated original sales and operating margin guidance, citing an unusually high number of Requests for Proposal (RFP) for security application deployments. However, since the Q1'10 conference call, a banking crisis and sovereign debt concerns have weighed on the Euro-zone. In our opinion, these issues could present significant headwinds for Vasco. First, recall that 68% of Q1'10 sales came from Europe. Further, 74% of sales came from banking. Third, since that time, the Euro has lost significant value versus the U.S. dollar. Lastly, we don't expect demand for OTP to remain high and expect Vasco to react to the changing market place by investing further in smart card credentialing authentication platforms. We believe expenses may remain elevated. Importantly, we don't believe the consensus estimates have been revised since the Q1'10 report, and we are concerned estimates may fall over the course of the next month or so. We have established FY'10 and FY'11 estimates below guidance and below the current consensus estimate. We forecast FY'10 sales/EPS of $112.7mm/$0.16, which compares to the $115.2mm/$0.22 consensus. Further, we forecast FY'11 sales/EPS of $129.5mm/$0.20, which compares to the $133mm/$0.31 consensus estimate.

Valuation and Price Target:

We have compared VDSI to a group of Vasco's peers, including OTP vendors, smart card vendors, full service identity management vendors, and enterprise security software vendors. We have found that, as a group, Vasco's peers trade at 2.3x forward sales, 2.5x book value, 15.1x forward earnings and a 7.1x Enterprise/EBITDA ratio. These valuation metrics imply a potential price target range of $3.01-$7.80 for shares of VDSI. Consistent with our coverage, we take the average of these potential targets to achieve a blended price target. Applying this to Vasco Data Security, we have established a $5.50 price target. With the stock trading within 10% of our target and supported by a solid balance sheet, we rate shares of VDSI a HOLD.

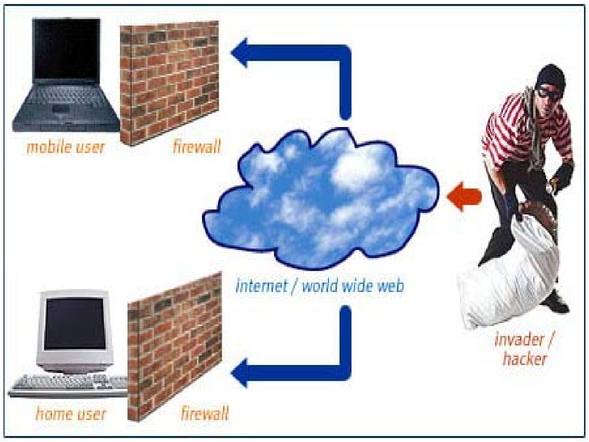
Device Authentication Overview

A world inside the computer where man has never been.
Never before now.
TRON
Enter its world this summer

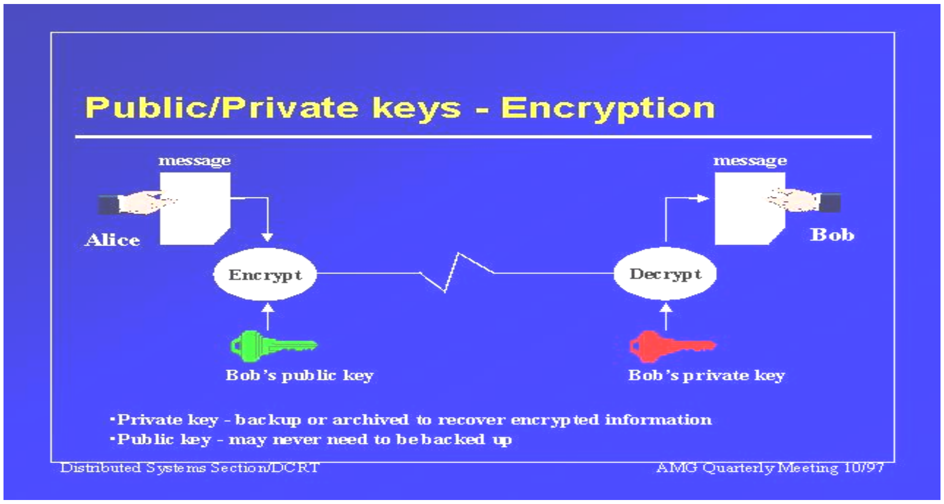
The modern secure credentialing and identification system is unique in that it forces the convergence of historically disassociated physical and logical access control applications. The new privilege authorization and access control platform authenticates devices and it authenticates people. This appendix describes various methods of authenticating devices and our opinions regarding their general viability. For our purposes, a device is anything that functions as a gateway or key representing access authorization to a logical domain or a physical domain. For example, a PC acts as a gateway between a human being and a logical domain or cyber space. Many different technologies serve as logical domain portals. PCs, smart phones, PDAs, laptops and game consoles all act as our gateways to the electronic dimension. Other devices serve as a key to unlock the domain portal device. Tokens, ID cards, storage devices and smart cards are good examples of logical domain portal keys. Conversely, ID cards, smart cards, proximity cards, PINS and traditional keys have historically represented physical access authorizations for doorways, gates, etc. Interestingly, both applications have utilized many of the same types of portal or keys, but have traditionally been completely separate. We believe those functions will converge into one basic key. We believe that the key (device) will ultimately be a smart card.

Logical Domain

We keep and do many important things in the logical domain. We store important information and property, we communicate with one another, we transact business and share property in the logical domain. These activities and things are valuable and, as such, are targeted by thieves and vandals. The logical domain is structured rather simply. There are places where things are stored and mediums that carry things from one place to another. Thieves steal from the places things are stored, or by intercepting things as they travel from one place to another. The most common form of securing the logical domain is a concept called Public Key Infrastructure (PKI). PKI uses firewalls, encryption (cryptography), and "keys" to perform basic security tasks. Firewalls keep everyone out. Encryption scrambles information into illegible secret code. Keys represent access authorization through the firewall or to descramble the communication. Access through the firewall or to the data is denied without a valid "Public Key." The public key is often referred to as a Certificate of Authority and is purposefully attached to the devices representing known and trusted people. The Certificate Authority (CA) performs the administration of PKI certificates. The CA associates valid certificates (keys) with authorized devices, which are associated with authorized users. The CA also manages the list of revoked or otherwise invalid certificates, called the Certificate Revocation List (CRL). Inbound devices, or data objects like email, verified by a valid certificate (public key), are accepted for interface.



Initiating Coverage of Vasco Data Security (VDSI) with a HOLD rating



Public/Private keys - Encryption

•Private key - backup or archived to recover encrypted information
•Public key - may never need to be backed up

Distributed Systems Section/DCRT

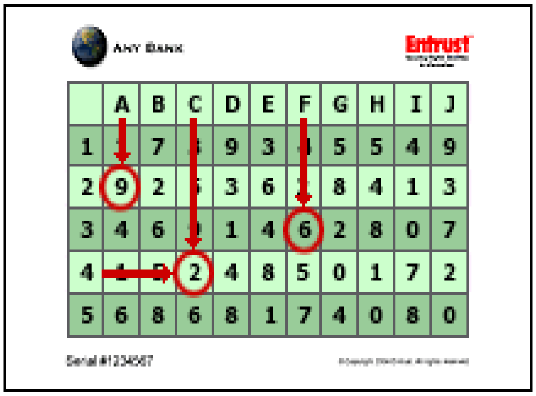
AMG Quarterly Meeting 10/97

The CA rejects inbound portal devices or objects not verified by a validated key. It's presumed that anyone using a keyed portal device is trusted and privileged. This fact, in our opinion, is the first of two major problems with PKI. First, PKI relies on false logic because, in reality, we don't care much about the device; we care about the person using the device. To the point, an unauthorized person could use an authorized device to gain unauthorized access. Second, PKI can become increasingly expensive over time as the CRL often grows, especially in large and dynamic organizations, requiring larger and more costly storage applications. As the CA and CRL grow, increasingly large lists of valid and revoked certificates must be centrally stored or downloaded to access control sites for comparison against incoming device keys. This storage/cost dynamic has propelled another offshoot PKI application called Online Certificate Status Protocol (OCSP). OCSP acts as an outsourced CRL. An access request prompts a certificate validation query to the OCSP server, which responds with "current," "expired" or "unknown," facilitating an acceptance or denial. Interesting companies providing CRL or OCSP solutions include CoreStreet, Inc., Tumbleweed Communications, and WidePoint.

In an attempt to close the false logic vulnerability, many device authentication vendors "personalize" the device by scrambling the public key and requiring a "Private Key," plus a PIN, to decode the "Public Key." If you don't have the PIN or password, you can't decrypt the public key. However, people are sometimes lazy, utilizing PINs or passwords that are easy to guess or simply listing them in public view: taped to their PC, for example. Attempting to close this vulnerability, device authentication vendors offered new, even more personalized keys called tokens in combination with random number (PIN/key) generator applets.

One-Time-Passcode Tokens

Tokens are simply yet another device, a small personal electronic device containing data, extending the device authentication false logic. Tokens serve as another key; one degree separated from the primary portal device, and are often designed to attach to a key ring, literally. Tokens interface with the portal devices, prompting for the PIN or private key. Thus, the token must be present to gain access. Some argue that tokens are an even more expensive way to extend and personalize the public key access privilege. Others argue that random key generators eliminate the important personalization (something you know). Recent attempts to overcome the price obstacle include simplifying the token by downloading the OTP generator applet to a cell phone, smart phone or PC replacing it with a wallet-sized card that contains a matrix of numbers or images. Upon access authorization request, the cardholder enters a PIN and is prompted to enter randomly selected numbers/images located in grid locations on the card. Without the card, the user would lack required data and be denied access. While this "bingo card" may reduce cost, it does nothing to reduce the false logic vulnerability beyond existing capabilities. We imagine users writing their PIN numbers, most likely their birth dates, on the bingo card before it's stolen or lost. Maybe they will tape the bingo card on the PC, right next to their PIN. "Access Approved!" Consequently, in our opinion, it simply cuts cost, which is why the



ANY BANK
Entrust

	A	B	C	D	E	F	G	H	I	J
1	[illegible]	7	8	9	3	4	5	5	4	9
2	9	2	5	3	6	[illegible]	8	4	1	3
3	4	6	9	1	4	6	2	8	0	7
4	[illegible]	[illegible]	2	4	8	5	0	1	7	2
5	6	8	6	8	1	7	4	0	8	0

Serial #1234567

financial community appears to endorse the concept. An interesting idea, but it doesn't really solve the security problem. We view it as a temporary patch or bridge.

Problems with One-Time-Passcode authentication models
We question the viability of One-Time-Passcode platforms (OTP) over the long-term for three distinct reasons. First, in our opinion, OTP is a system that relies on false logic, implying that the presentation of an OTP reasonably assures that the legitimately entitled privilege holder actually executed the command to generate the password. In other words, modern OTP platforms rely on the presumption that the person pressing the token button is the rightful owner of the OTP token. Since it cannot always be reasonably assured that the legitimate OTP was generated by the legitimate owner of the token, the OTP itself is little more secure than a standard password/PIN platform. In fact, most OTP platforms provide the option to include a password/PIN system in combination with the OTP to help verify the holder of the token. This is often described as "two factors" or even "strong authentication", requiring both something held by the authorized person and something known by that person. Thus, without the password/PIN, the presentation of an OTP really only ensures that a valid OTP generator was present at the time of the transaction. The password/PIN authenticates the user; the token does not.

Second, distinct OTP systems typically don't interoperate or cross-authenticate competing tokens. Thus, services seeking stronger authentication using tokens must ask customers to use a specific vendor's token. Unless that token is registered in competing OTP platforms, consumers may need multiple tokens to authenticate themselves for various distinct services. This is a major hassle factor that has caused OTP vendors to cross certify their systems. This cross certification effectively renders all OTP platforms equivalent, leaving price the only competitive advantage. Thus, it's not surprising that OTP platform vendors like Verisign, RSA (EMC), ActivIdentity, SafeNet, Aladdin and Vasco now offer the opportunity to download a free OTP generator to the desktop or smart phone, in lieu of the token. This lowers cost. Yet, deployed this way, the OTP generator actually only serves as another form or layer of device authentication, which is exactly what digital certificates and Public Key Infrastructure does. Since most PCs, laptops, cell and smart phones are issued fully enabled with some type of PKI certificates to authenticate the devices before they are allowed to access a network, there really isn't any reason to use an OTP embedded in the device along side the certificate. Further, PKI vendors today have started selling their Certificate Authority validation capabilities as a subscription service, dramatically lowering the up front cost of deploying PKI.

Lastly, since 9/11, standards development groups for the identity management and credentialing industries have focused on PKI and biometrically enabled smartcard systems. Those standards and specifications don't require OTP. Thus, we aren't surprised to find rapid price compression and slowing growth rates in OTP. In our opinion, OTP is ultimately destined for the museum. We predict that PKI enabled contactless smart card credentials, in various form factors, will become pervasive along with biometrics. Various form factors will include smart card IDs, like driver's licenses and credit cards, as well as SIM card enabled smart phones. It is the biometric that ultimately will authenticate the rightful owner of the credential. Thus, the device is authenticated by PKI and the user is authenticated by the biometric.

WHAT IS PERSONAL IDENTITY VERIFICATION (PIV) AND FIPS201?

At the most rudimentary level, a modern PIV system performs two basic tasks. It approves good people and rejects bad people. From another view, the application **identifies** safe people and **verifies** their identity as they approach. Anyone else is presumed to be bad and is denied. It answers the questions **"Who are you?" "Are you someone we will grant access to?"** and then **"Are you who you say you are?"** However, it's not all that simple because we must establish access control privileges for **physical access control** (doors, gates, borders, etc.) and also **logical access control** (computers, networks, internet, etc.). Historically, we separated the two authentication functions, attempting to automate those using completely independent technologies.

Physical Access Control Systems (PACS)

We controlled physical domains by **authenticating a person**. We historically authenticated "friends" by remembering what they look and sound like. By definition, we relied on a **biometric**, a personally unique physiological attribute. We have automated biometric authentication with fingerprints, faces, irises, or hand-bone geometries, among others. Biometrics is used in **Physical Access Control Systems**. However, these technologies, on the whole, were underdeveloped and technically incapable of performing the desired tasks well enough to warrant their expense. Moreover, conceptually, biometric applications can be politically, culturally or socially unpopular, especially in the United States. Consequently, demand for such systems remained relatively low, depressing research investment, at least until after 9/11.

Logical Access Control (LACS)

Conversely, we attempted to control logical domains by **authenticating a device.** After all, people don't physically enter a computer network. People loosely interface with a logical domain through a personal computer or other portal device like a cell phone, PDA, etc. These systems are **Logical Access Control Systems** and answer the question **"Is this device allowed to interface with our device or system?"** One widely recognized device authentication application is **public key infrastructure** (PKI). It's presumed that anyone using an authenticated device is acceptable. However, controlling logical domains by authenticating and verifying the approaching device relies on false logic because, in reality, **we don't care much about the device; we care more about the person using the device**. To the point, an unauthorized person could use an authorized device to gain unauthorized access. Of course, "hacking" is a huge problem and we believe the obvious gravity of the hacking problem today is testament enough to the inadequacy of exclusive reliance on device authentication for logical access control, or any access control. Ironically, the modern solution strives to incorporate both PACS' and LACS' functionality into the same platform, **authenticating the device and the person for every access control transaction**. Thus, modern access control thinking proposes to accomplish these tasks by combining distinct and previously exclusive technologies into a symbiotic system. These technology capabilities allow the stakeholder to perform four core functions: a) **identity basis**, b) **privilege entitlement and life cycle management**, c) **issuance and distribution**, and d) **access control**.

Why is PIV important?

Because we can no longer trust that you are who you say you are.

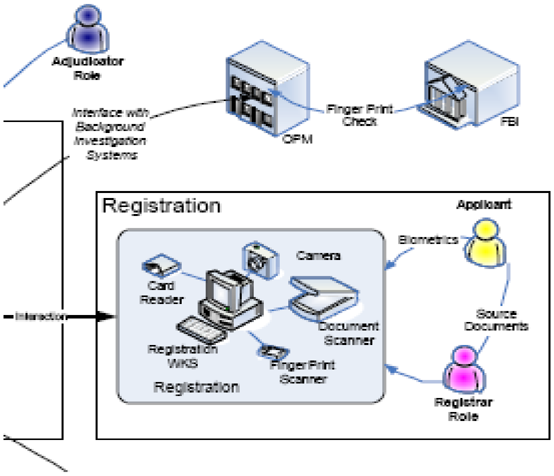
The 9/11 tragedies exemplified risks with insufficient credentialing and access control, while identity theft and fraud are pervasive, costing society billions annually. The FTC estimated identity theft victims in the year ending in May 2003 totaled 9.91 million individuals, with losses totaling $52.6 billion ($47.6 billion to businesses and $5 billion to individual victims). E-communication and e-commerce have only amplified our credentialing vulnerabilities. Our applications to establish or maintain trust are broken.

International and domestic governments have re-examined global credentialing, privileging, and access control systems. Significant research and development has produced new technology standards, application profiles and best practices, which are visible today. Those standards are now required by both international and domestic (U.S.) law for implementation in critical infrastructure industries.

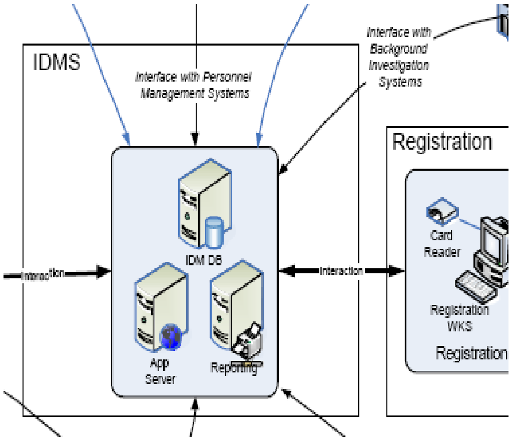
Therefore, we believe demand for advanced credentialing management systems will grow relatively rapidly over the coming years. We believe advanced credentialing capabilities will displace less sophisticated and less expensive systems as government mandates take effect in critical infrastructure industries like banking, energy, healthcare, transportation and telecommunications.

Identity Basing

"Who are you? Who aren't you? How do we know?" Identity basing refers to the process of determining who would receive a privilege authorization and credential. Logically, it's part of a Registration or enrollment process. Also known as proofing or vetting, the goal is to ensure access authorization is not granted to potentially dangerous people. Failing to prevent cancerous entries into the pool of privileged individuals compromises the integrity of the entire secure credentialing and access control system. For example, accidentally providing Al Qaeda operatives with complete access to Federal Reserve facilities could be a problem. The process of identity basing can vary, but typically involves capturing a series of unique personal identifiers, including biographic, demographic, and/or biometric data, and screening those identifiers against lists or databases containing similar identifiers from known individuals. The more data captured, the more robust the screen's potential. Society doesn't maintain significant datasets of identifiers associated with "good" people, at least not yet. Society does maintain significant datasets of identifiers associated with "bad" people. For example, large databases of criminal fingerprints exist for these purposes. Consequently, today, identity basing, proofing, or vetting compares applicant data with similar data from potentially bad people, to ensure the applicant is NOT a bad person. Of course, "criminal background checks" have negative connotations. Fortunately, the depth of the vetting process can be gauged relative to the security sensitivity of the applied-for privilege. A discount buyer club membership may not require a criminal background check, while Pentagon access privileges might. Moreover, most privileges are applied for, implying a voluntary submission to checks. This gives the applicant some privacy control, as they can "opt in" or "opt out."

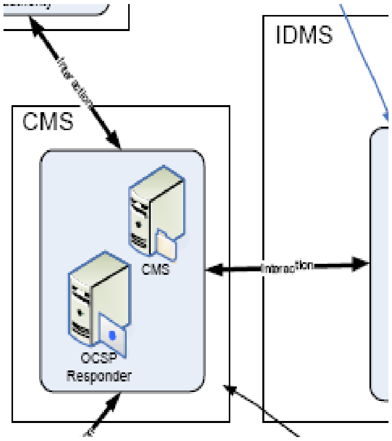


Today, our primary data screens for vetting purposes are alphanumeric and biometric. While alphanumeric searches are relatively simple, biometric searches for background screening are potentially very complex. Two biometrics—fingerprints and faces—dominate and will continue to dominate, the identity basing function. In our opinion, Cogent Systems L1 Identity, Sagem MorphoTrak, and CrossMatch are interesting companies in this area. Moreover, the public and the street seem to vastly misunderstand biometrics, its applications and capabilities.



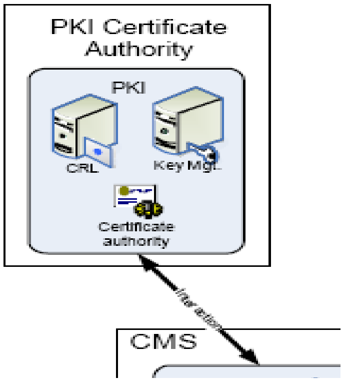
Privilege Entitlement and Life Cycle Management

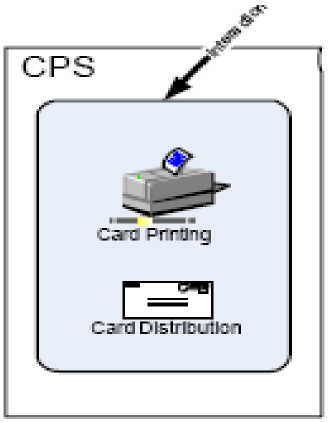
"Where can they go? What can they do?" We loosely associate Privilege Entitlement and Life Cycle management with Identity Basis because access control privileges are likely predetermined. Identity Basing simply qualifies the applicant to receive the predetermined privileges being applied for. Privilege Entitlement is primarily a clerical function. The Identity Management System (IDMS) associates access control privileges with an identity. It's populated with data, potentially applicant data, ID numbers and related access entitlements. Biometric, demographic, or biographic data need not, but could be stored in the IDMS. The IDMS administrates identity life cycles and serves as a clearinghouse, linking a known identity with pre-established access control entitlements. As identity status changes, including entitlements, the IDMS administrates necessary instructions and execution of those updates. The IDMS interfaces with virtually all other system components. Once the IDMS is populated, the Card Management System (CMS) associates an ID card, the device, with the identity from the IDMS. Like the IDMS, the CMS is basically a clerical application. It's a clearinghouse that associates an established identity with a device and logical domain access entitlements with the device. It does not directly associate intimate personal information or logical domain access entitlements with the person. The CMS also manages card life cycles, administrating and executing card updates and forwarding logical access entitlement updates. In our opinion, IDMS and CMS applications require significant entitlement and distribution expertise, but don't require substantial intellectual property. Existing, large IT system integrators will likely provide these applications. We believe vendors providing other system components will likely begin to provide overlapping IDMS and CMS capabilities as value-added features in addition to their core capabilities. To this end, the business and investment case for stand-alone IDMS/CMS functions is relatively weak, in our opinion. Notable companies in this area include L1 Identity, ActiveIdentity Corp., Lockheed Martin Corp., Daon Corp, Northrop Grumman, Unisys, Bearing Point, Anteon Corp, Bell-ID Corp, and Lenel Security Corp.



Privilege and Credential Issuance and Management

Please recall the discrepancies between PACS and LACS. Like people, ID cards (a device) cannot be forced into a logical domain. However, we can authenticate a thing that serves as an interface between the logical domain and the authorized person. Today, the primary method of authenticating a device is called Public Key Infrastructure (PKI). PKI utilizes encryption, or cryptography, to scramble data sent within a private communication. The data cannot be reconstituted without access to a "Public Key." The public key is often referred to as a Certificate of Authority and is purposefully attached to the devices representing known and trusted people. The PKI Certificate Authority (CA) performs the administration of PKI certificates. The CA associates valid certificates (keys) with authorized devices. In this case, the authorized device is the smart ID card. Inbound devices, or data objects like an email, represented by a valid certificate (public key), are accepted for interface. The CA rejects inbound devices/objects lacking a Certificate (key) or producing an invalid key. Scrambling the public key and requiring a "Private Key," plus a PIN, to decode the "Public Key" can reinforce the Public Key/Certificate. In our opinion, vendors deserving attention include VeriSign, ActivIdentity, Entrust, RSA Security, SafeNet, Tumbleweed Communications, WidePoint and CoreStreet. With Identity Basis established and both physical and logical access entitlements authorized, the CMS can instruct the Card Printing System (CPS) to produce and distribute the credential. The CPS can print in a centralized environment with arrays of printers in one location, or in a distributed environment with individual printers located in remote locations, potentially attached to a Wide Area Network (WAN). Importantly, not all card printers are created equally and the competitive field is stratified by technology sophistication. We believe Fargo Electronics, Zebra Technology and DataCard Group represent "Best of Breed" in credentialing printers



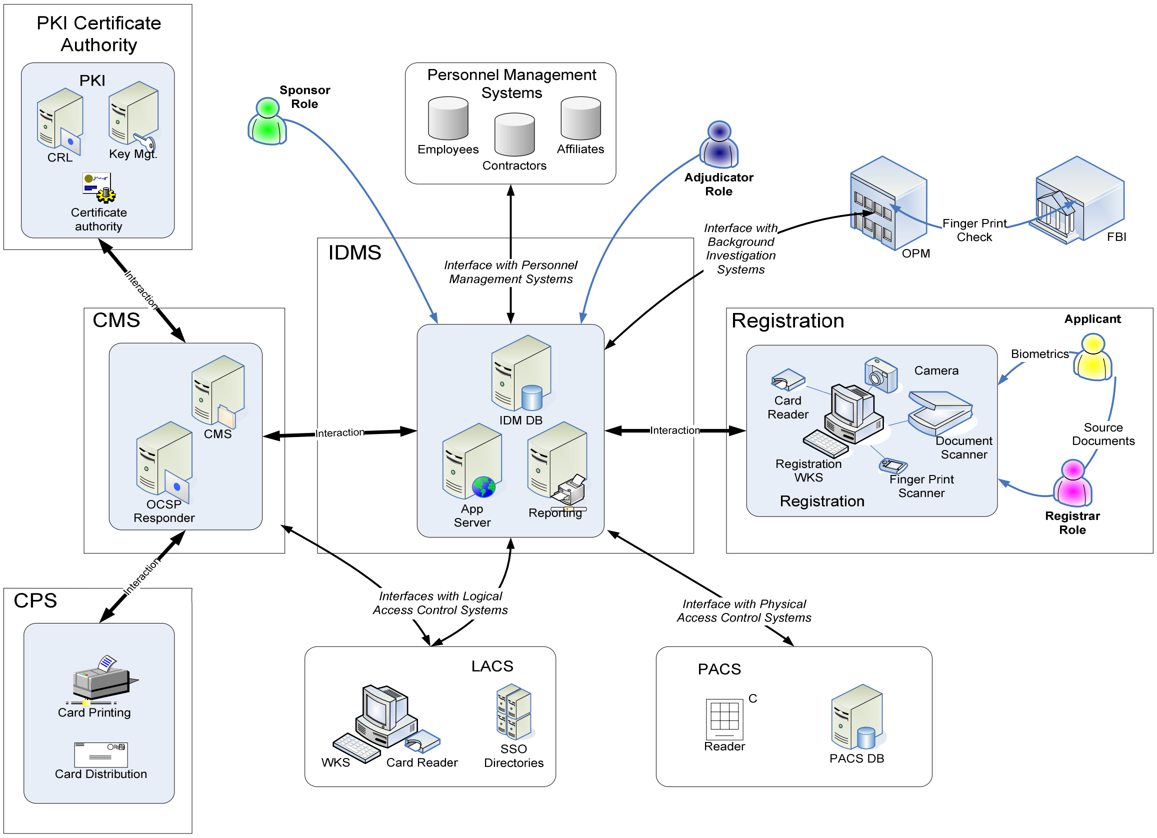


Federal Information Processing Standard #201 (FIPS201)

FIPS201 is the Federal Governments specification governing Federal Identity Management policies and procedures. It is important because it is the first large-scale credentialing/access controls implementation requiring open platforms, technology standards and best practices for every component, process and application. It seems highly likely the FIPS201 model will be globally accepted. However, while adopting a “standardized” and “interoperable” technology ultimately reduces purchaser risk, there is some risk in standardizing on specific technology applications, especially applications that are relatively new and likely to evolve. Technology standards, once fixed, cannot be easily altered. In fact, in some cases they cannot be changed for five years. Consequently, we risk the technology “state-of-the-art” being several years advanced from the “state of the market”, but with virtually no market viability. Because the technology base continues to evolve, FIPS201 is designed for flexibility with respect to underlying technology components. FIPS201 acts as an envelope containing various shorter-term specifications called Special Publications (SP-800) that can be altered or refreshed every six months.

FIPS201 consists of two parts, and more could be coming. The two parts are PIV-1 and PIV-2. The standards in PIV-1 describe and support all the of the security requirements set forth in HSPD-12. PIV-2 includes standards that describe technical interoperability requirements described in HSPD-12. PIV-2 further lays out standards for implementing smart ID cards. Federal Information Processing Standard #201 (FIPS201) uses the Federal Smart Card Interoperability Specification, ver. 2.1, and related documentation as its basis. NIST Special Publication 800-73 (SP800-73), “Interfaces for Personal Identity Verification” specifies the interface and data elements of the PIV card. NIST Special Publication 800-76 (SP800-76), “Biometric Data Specification for Personal Identity Verification” specifies the technical acquisition and formatting requirements for biometric data of the PIV system. NIST Special Publication 800-78 (SP800-78), “Cryptographic Algorithms and Key Sizes for Personal Identity Verification” specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system. NIST Special Publication 800-79 (SP800-79), “Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations” outlines qualifications for entities required to distribute PIV cards. NIST Special Publication 800-85 (SP800-85), “PIV Middleware and PIV Card Application Conformance Test Guidelines” specifies testing processes vendors must utilize to validate their products compliance with interoperability specifications. Finally, NIST Special Publication 800-87 (SP800-87), “Codes for the Identification of Federal and Federally-Assisted Organizations” outlines what qualifies an entity for inclusion under HSPD-12, compelling them to comply with FIPS201. NIST Special Publication 800-96 (SP800-96) outlines technology standards required for contact and contactless smart card readers.

HSPD-12 Core Components



September year-end	Fiscal	Fiscal	Fiscal	Q1	Q2	Q3	Q4	Fiscal	Q1	Q2E	Q3E	Q4E	Fiscal	Fiscal
(in thousands)	2006	2007	2008	Mar-09	Jun-09	Sep-09	Dec-09	2009	Mar-10	Jun-10	Sep-10	Dec-10	2010E	2011E
TOTAL SALES	**76,062**	**119,980**	**132,977**	**23,175**	**24,458**	**22,126**	**31,936**	**101,695**	**23,915**	**27,246**	**26,109**	**35,449**	**112,719**	**129,511**
Cost of Goods	24,359	40,868	41,007	6,477	7,746	6,736	9,577	**30,536**	7,227	8,446	7,722	10,989	**34,384**	**40,449**
GROSS PROFIT	**51,703**	**79,112**	**91,970**	**16,698**	**16,712**	**15,390**	**22,359**	**71,159**	**16,688**	**18,800**	**18,387**	**24,460**	**78,335**	**89,063**
Margin %	*68.0%*	*65.9%*	*69.2%*	*72.1%*	*68.3%*	*69.6%*	*70.0%*	*70.0%*	*69.8%*	*69.0%*	*70.4%*	*69.0%*	*69.5%*	*68.8%*
Expenses:														
Selling	19,482	27,181	35,352	6,802	8,033	6,767	8,439	30,041	7,929	8,786	8,700	10,800	36,215	40,544
%	*25.6%*	*22.7%*	*26.6%*	*29.4%*	*32.8%*	*30.6%*	*26.4%*	*29.5%*	*33.2%*	*32.2%*	*33.3%*	*30.5%*	*32.1%*	*31.3%*
R&D	5,529	9,440	11,618	2,444	3,017	2,820	3,301	11,582	3,272	3,726	3,500	5,000	15,498	18,100
%	*7.3%*	*7.9%*	*8.7%*	*10.5%*	*12.3%*	*12.7%*	*10.3%*	*11.4%*	*13.7%*	*13.7%*	*13.4%*	*14.1%*	*13.7%*	*14.0%*
G&A	7,157	10,569	16,237	2,623	4,200	3,734	5,114	15,671	4,648	4,750	4,500	4,850	18,748	20,940
%	*9.4%*	*8.8%*	*12.2%*	*11.3%*	*17.2%*	*16.9%*	*16.0%*	*15.4%*	*19.4%*	*17.4%*	*17.2%*	*13.7%*	*16.6%*	*16.2%*
Total Non-Cash OpEx	*593*	*1,029*	*626*	*107*	*110*	*115*	*121*	*453*	*115*	*123*	*127*	*123*	*487*	*529*
Total Operating Expenses	32,761	48,219	63,833	11,976	15,360	13,436	16,975	57,747	15,964	17,385	16,827	20,773	70,949	80,113
%	43.1%	40.2%	48.0%	51.7%	62.8%	60.7%	53.2%	56.8%	66.8%	63.8%	64.4%	58.6%	62.9%	61.9%
OPERATING INCOME	**18,942**	**30,893**	**28,137**	**4,722**	**1,352**	**1,954**	**5,384**	**13,412**	**724**	**1,415**	**1,560**	**3,687**	**7,386**	**8,950**
Margin %	*24.9%*	*25.7%*	*21.2%*	*20.4%*	*5.5%*	*8.8%*	*16.9%*	*13.2%*	*3.0%*	*5.2%*	*6.0%*	*10.4%*	*6.6%*	*6.9%*
Interest Income	121	479	990	143	165	73	191	572	71	120	109	114	414	684
Other Income (expense)	(422)	(384)	(209)	(248)	1,206	530	618	2,106	60	446	331	323	1,160	1,527
PRETAX INCOME	**18,641**	**30,988**	**28,918**	**4,617**	**2,723**	**2,557**	**6,193**	**16,090**	**855**	**1,981**	**2,001**	**4,124**	**8,961**	**11,161**
Margin %	*24.5%*	*25.8%*	*21.7%*	*19.9%*	*11.1%*	*11.6%*	*19.4%*	*15.8%*	*3.6%*	*7.3%*	*7.7%*	*11.6%*	*7.9%*	*8.6%*
Income Tax Provision	6,054	10,025	4,627	1,154	681	1,035	589	3,459	282	653	660	1,360	2,956	3,681
Minority Interest	-	-	-	-	-	-			-	-	-	0		
NET INCOME	**12,587**	**20,963**	**24,291**	**3,463**	**2,042**	**1,522**	**5,604**	**12,631**	**573**	**1,328**	**1,341**	**2,764**	**6,005**	**7,480**
Margin %	*16.5%*	*17.5%*	*18.3%*	*14.9%*	*8.3%*	*6.9%*	*17.5%*	*12.4%*	*2.4%*	*4.9%*	*5.1%*	*7.8%*	*5.3%*	*5.8%*
EPS Reported	**$0.33**	**$0.55**	**$0.64**	**$0.09**	**$0.05**	**$0.04**	**$0.15**	**$0.33**	**$0.01**	**$0.03**	**$0.04**	**$0.07**	**$0.16**	**$0.20**
Shares Average	37,765	38,258	38,204	38,022	38,091	38,154	38,068	38,084	38,287	38,124	38,134	38,144	38,155	38,205
EBITDA	**0.52**	**0.83**	**0.75**	**0.13**	**0.04**	**0.05**	**0.14**	**0.36**	**0.04**	**0.08**	**0.09**	**0.20**	**0.41**	**0.50**
Assets														
Current Assets:														
Cash & mktable securities	14,768	38,833	57,714	57,329	67,589	71,230	67,601	67,601	76,120	77,513	77,309	83,059	83,059	87,325
Acct receivables, net	19,617	25,721	24,951	21,558	17,402	20,404	31170	31,170	21,979	22,000	21,000	26000	26,000	24,600
Inventories, net	4,275	7,076	13,376	12,857	12,321	10,222	9015	9,015	8,904	10,500	11,000	11500	11,500	14,200
Other	2,660	7,287	9,861	3,822	3,304	3,680	4361	4,361	3,165	4,489	4,689	4887.9	4,888	5,685
Total current assets	41,320	78,917	105,902	95,566	100,616	105,536	112,147	112,147	110,168	114,502	113,998	125,447	125,447	131,810
Restricted Cash			0	0	0	0	0		0	0	0	0		
Investments		0	0	-	-	-	0	0	-	-	-	0	0	0
Property, Plant & equip.	1,422	2,140	4,176	4,396	4,822	5,287	5,189	5,189	4,947	4,601	4,279	3,979	3,979	4,585
Intangible assets, net	3,013	2,295	1,997	1,875	1,885	1,873	1,797	1,797	1,706	1,587	1,476	1,372	1,372	1,027
Other assets	4,206	3,005	2,291	1,789	1,494	1,132	548	548	970	1,650	1,450	1200	1,200	950
Goodwill	12,685	14,319	13,584	12,726	13,537	14,044	13813	13,813	12,967	12,967	12,967	12967	12,967	12,967
Total Assets	62,646	100,676	127,950	116,352	122,354	127,872	133,494	133,494	130,758	135,306	134,169	144,966	144,966	151,339
Liab. & Shr. Equity		0	0					0					0	0
AP	7,579	7,757	10,349	4,986	4,193	3,885	4,505	4,505	4,287	4,800	4,400	5,500	5,500	6,230
Accrued Compensation	3,176	5,330	5,780	4,317	4,821	5,177	5,178	5,178	5,141	5,902	6,196	6,490	6,490	7,665
Current portion of debt	2,154	0	0	-	-	-	-	0	-	-	-	-	0	0
Accrued and other Current Lia	4,272	7,784	7,962	5,638	6,075	7,434	6,382	6,382	6,559	7,639	7,998	8,357	8,357	9,794
Current portion of Deferred R	2,081	5,608	5,881	5,373	5,589	5,719	7,188	7,188	7,862	7,919	8,476	9,034	9,034	11,264
Total current Liabilities	19,262	26,479	29,972	20,314	20,678	22,215	23,253	23,253	23,849	26,260	27,070	29,381	29,381	34,953
Deferred Revenue	302	766	888	710	578	410	277	277	185	211	202	274	274	313
Long- Term Acc for Restructu	0	0	0	-	-	-	-	0	-	-	-	-	0	0
Long Term Deferred Rent	0	0	0	-	-	-	-	0	-	-	-	-	0	0
Other	876	600	1,806	261	381	548	818	818	925	1,145	1,329	1,513	1,513	2,248
Minority Interest	0	0	0	-	-	-	-	0	-	-	-	-	0	0
Total Liabilities	20,440	27,845	32,666	21,285	21,637	23,173	24,348	24,348	24,959	27,616	28,601	31,168	31,168	37,513
Stockholder's equity	42,206	159,443	95,284	95,067	100,717	104,699	109,146	109,146	105,799	107,691	105,568	113,798	113,798	113,826
Total Liabs. & SE	62,646	187,288	127,950	116,352	122,354	127,872	133,494	133,494	130,758	135,306	134,169	144,966	144,966	151,339
Balance Sheet Ratios														
Cash Per Share (avg)	$ 0.39	$ 1.02	$ 1.51	$ 1.51	$ 1.77	$ 1.87	$ 1.78	$ 1.78	$ 1.99	$ 2.03	$ 2.03	$ 2.18	$ 2.18	$ 2.29
Book value (avg shares)	$ 1.12	$ 4.17	$ 2.49	$ 2.50	$ 2.64	$ 2.74	$ 2.87	$ 2.87	$ 2.76	$ 2.82	$ 2.77	$ 2.98	$ 2.98	$ 2.98
Tangible book value (avg shar	$ 1.04	$ 4.11	$ 2.44	$ 2.45	$ 2.59	$ 2.70	$ 2.82	$ 2.82	$ 2.72	$ 2.78	$ 2.73	$ 2.95	$ 2.95	$ 2.95
Working capital	$21,756	$51,672	$75,042	$74,542	$79,360	$82,911	$88,617	$88,617	$86,134	$88,032	$86,726	$95,793	$95,793	$96,545
Current ratio	2.1	3.0	3.5	4.7	4.9	4.8	4.8	4.8	4.6	4.4	4.2	4.3	4.3	3.8
Debt/total cap	0.5%	0.4%	0.7%	0.6%	0.5%	0.3%	0.2%	0.2%	0.1%	0.2%	0.2%	0.2%	0.2%	0.2%
Days Sales	93	77	68	84	64	83	88	110	83	73	72	66	83	68
Inv turns	1.0x	4.2x	2.5x	1.8x	2.0x	2.2x	3.5x	2.8x	2.7x	2.6x	2.4x	3.1x	2.5x	2.3x
Days Payable	35.87	23.27	28.02	19.36	15.43	15.80	12.70	15.95	16.13	15.86	15.17	13.96	17.57	17.32

June 8, 2010 **Comp Table**

		(prev clos	Market	NY	Px/	Shares	Book	Px/	First Call - EPS Estimates			5yr	Operating	P/E			EBITDA			Enterprise	EV/EBITDA		
Ticker	Company Name	Price	Value	Revenue	Sales	Out	Value	Book	Trail	TY	NY	Growth	Margin	Trail	TY	NY	Trail	TY	NY	Value	Trail	TY	NY
HPQ	HEWLETT PACKARD CO	45.2375	106,086.1	130,937.5		2,345.1	18.41	2.5	4.28	4.50	4.97	7.00	9.12	10.6	10.1	9.1	15,798.0	18,341.1	19,704.2	106,026.14	6.7	5.8	5.4
EMC	EMC CORPORATION MASS	18.03	37,062.6	18,297.7	2.03	2,055.6	7.76	2.3	1.05	1.20	1.36	11.06	10.85	17.2	15.1	13.2	3,518.4	4,478.1	4,512.0	33,467.56		7.5	7.4
MSFT	MICROSOFT CORP	25.29	221,637.5	67,066.8	3.30	8,763.8	5.64	4.5	2.05	2.05	2.31	18.00	35.90	12.4	12.4	10.9	23,161.0	25,788.5	27,921.4	193,936.49	8.4	7.5	6.9
VRSN	VERISIGN INC	27.66	5,047.9	1,202.2	4.20	182.4	3.28	8.4	1.41	1.54	1.74	7.50	32.01	19.6	17.9	15.9	460.6	523.9	577.6	4,144.89	9.0	7.9	7.2
MFE	MCAFEE INC	31.73	4,950.5	2,312.3	2.14	156.0	13.41	2.4	2.50	2.58	2.89	10.67	12.25	12.7	12.3	11.0	588.0	694.8	756.9	4,049.64	6.9	5.8	5.4
CHKP	CHECK POINT SOFTWARE TE	29.85	6,197.5	1,126.7	5.50	261.2	42.08	0.7	2.18	2.31	2.51	10.40	45.88	13.7	12.9	11.9	514.6	542.8	577.5	2,844.44	5.5	5.2	4.9
CUB	CUBIC CORPORATION	33.77	902.9	1,131.2	0.80	26.7	17.05	2.0	2.26	2.35	2.43	17.00	8.33	15.0	14.4	13.9	100.3	106.0	111.7	671.24	6.7	6.3	6.0
ID	L-1 IDENTITY SOLUTIONS INC	7.17	665.9	806.9	0.83	92.9	7.90	0.9	(0.02)	0.03	0.17	9.50	5.40	na	286.8	42.2	72.3	101.5	120.6	1,078.55	14.9	10.6	8.9
OTIV	OTI ON TRACK INNOVATIONS	1.99	39.6	60.2	0.66	23.9	4.75	0.4	(0.36)	0.01	0.28	10.50	(44.70)	na	199.0	7.1	(10,851.0)	(109.0)	--	39.58	(0.0)	(0.4)	
ACTI	ACTIVIDENTITY CORPORATIC	2.15	103.4	78.2	1.32	48.1	1.96	1.1	(0.04)	0.01	0.14	11.50	(11.54)	na	430.0	15.4	--	2.0	8.8	103.38		51.7	11.7
				0.0	2.31			2.52				11.31		14.44		15.05							7.10
				0.0																			
VDSI	**VASCO DATA SECURITY INTL**	**5.94**	**227.5**	**129.5**	**1.76**	**38.3**	**2.76**	**2.2**	**0.27**	**0.16**	0.20	**13.00**	**12.43**	**22.3**	**37.1**	**29.7**	**2.3**	**15.6**	19.1	**159.90**		**10.3**	**8.4**
Px Tgt Implied by Group Ave:					$7.80			$6.95								$3.01							$3.54

Ave. Px Target applied to VDSI: **$ 5.33**

Analyst Certification

I, Jay M. Meier, certify that the views expressed in this research report accurately reflect my personal views about the subject company and its securities. I also certify that I have not been, am not, and will not be receiving direct or indirect compensation related to the specific recommendations expressed in this report.

Important Disclosures:

The analyst or a member of his/her household **does not** hold a long or short position, options, warrants, rights or futures of this security in their personal account(s).

As of the end of the month preceding the date of publication of this report, Feltl and Company **did not** beneficially own 1% or more of any class of common equity securities of the subject company.

There **is not** any actual material conflict of interest that either the analyst or Feltl and Company is aware of.

The analyst **has not** received any compensation for any investment banking business with this company in the past twelve months and **does not** expect to receive any in the next three months.

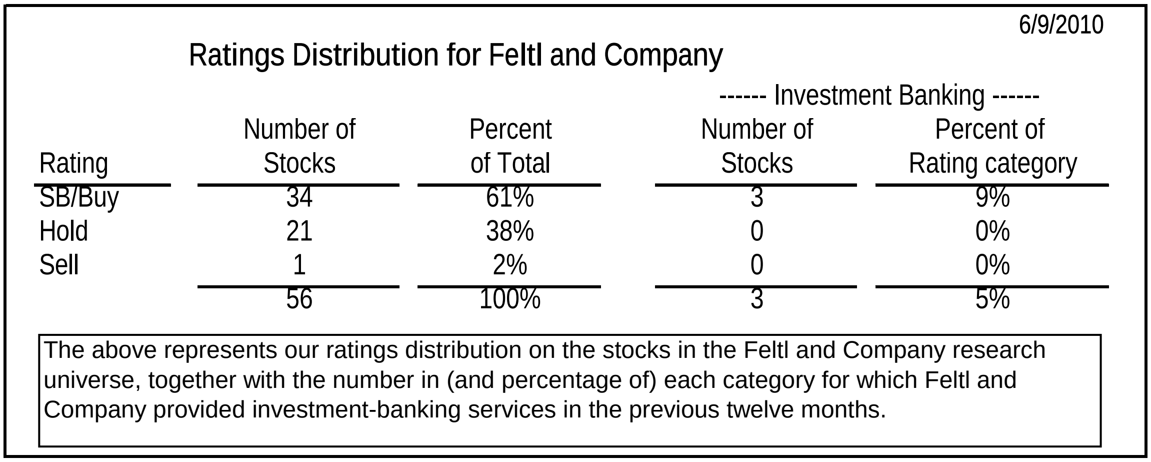
Feltl and Company **has not** been engaged for investment banking services with the subject company during the past twelve months and **does not** anticipate receiving compensation for such services in the next three months.

Feltl and Company **has not** served as a broker, either as agent or principal, buying back stock for the subject company's account as part of the company's authorized stock buy-back program in the last twelve months.

No director, officer or employee of Feltl and Company serves as a director, officer or advisory board member to the subject company.

Feltl and Company Rating System: Feltl and Company utilizes a four tier rating system for potential total returns over the next 12 months.

Strong Buy: The stock is expected to have total return potential of at least 30%. Catalysts exist to generate higher valuations, and positions should be initiated at current levels.
Buy: The stock is expected to have total return potential of at least 15%. Near term catalysts may not exist and the common stock needs further time to develop. Investors requiring time to build positions may consider current levels attractive.
Hold: The stock is expected to have total return potential of less than 15%. Fundamental events are not present to make it either a Buy or a Sell. The stock is an acceptable longer-term holding.
Sell: Expect a negative total return. Current positions may be used as a source of funds.

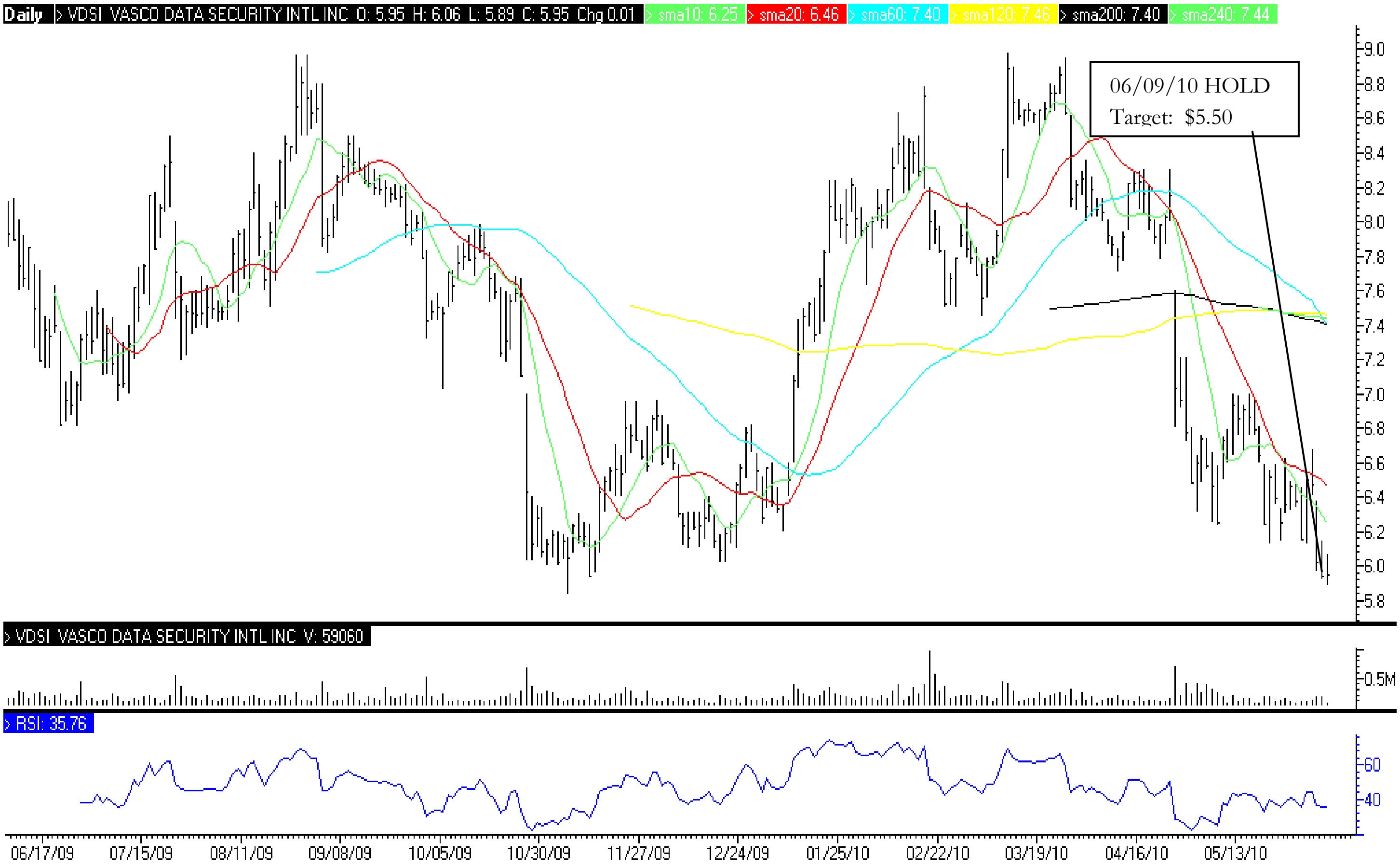


6/9/2010

Ratings Distribution for Feltl and Company

			------ Investment Banking ------	
Rating	Number of Stocks	Percent of Total	Number of Stocks	Percent of Rating category
SB/Buy	34	61%	3	9%
Hold	21	38%	0	0%
Sell	1	2%	0	0%
	56	100%	3	5%

The above represents our ratings distribution on the stocks in the Feltl and Company research universe, together with the number in (and percentage of) each category for which Feltl and Company provided investment-banking services in the previous twelve months.



Date	Nature of Report	Rating	Price Target
06/09/10	Initiation@$5.83	HOLD	$5.50

Feltl and Company **does** make a market in the subject security at the date of publication of this report. As a market maker, Feltl and Company could act as principal or agent with respect to the purchase or sale of those securities.

Valuation and Price Target Methodology:

We have compiled a group of Vasco's peers, including OTP vendors, smart card vendors, full service identity management vendors, and enterprise security software vendors. We have found that, as a group, Vasco's peers trade at 2.3x forward sales, 2.5x book value, 15.1x forward earnings and a 7.1x Enterprise/EBITDA ratio. These valuation metrics imply a potential price target range of $3.01-$7.80 for shares of VDSI. Consistent with our coverage, we have averaged these potential targets to achieve a blended price target. Applying this to Vasco Data Security, we have established a $5.50 price target. With the stock trading within 10% of our target and supported by a solid balance sheet, we rate shares of VDSI a HOLD.

Risks to Achievement of Estimates and Price Target:

- Actual or anticipated fluctuations in operating results.
- Announcements of technological innovations.
- New products introduced by, or new contracts entered into by the Company or competitors.
- Competition.
- Developments with respect to intellectual property.
- Changes in demand for security software applications in general.
- Changes in the general economic or market conditions, including the impact of foreign exchange rates.
- Readers should recognize that the risks noted here do not represent a comprehensive list of all risk factors or potential issues, nor all factors that may preclude achievement of our forecast or price target. Additional risk factors exist and are outlined the Company's SEC filings.

Other Disclosures:

The information contained in this report is based on sources considered to be reliable, but not guaranteed, to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of this date, and are subject to change without notice. This report has been prepared solely for informative purposes and is not a solicitation or an offer to buy or sell any security. The securities described may not be qualified for purchase in all jurisdictions. Because of individual requirements, advice regarding securities mentioned in this report should not be construed as suitable for all accounts. This report does not take into account the investment objectives, financial situation and needs of any particular client of Feltl and Company. Some securities mentioned herein relate to small speculative companies that may not be suitable for some accounts. Feltl and Company suggests that prior to acting on any of the recommendations herein, the recipient should consider whether such a recommendation is appropriate given their investment objectives and current financial circumstances. Past performance does not guarantee future results. Additional information is available upon request.

Equity Capital Markets
Directory

Feltl and Company
SECURITIES BROKERAGE AND INVESTMENT BANKING

Research Department

Brent R. Rystrom
Director of Equity Research
(612) 492-8810

Ernest W. Andberg, CFA
(612) 492-8836

Jay M. Meier
(612) 492-8847

Mark E. Smith
(612) 492-8806

Joshua J. Elving
(612) 492-8872

Scott R. Berg
(612) 492-8857

Shawn P. Bitzan
(612) 492-8816

Trading: (866) 777-9862

William W. Koop
Director of Equity Trading
(612) 492-8830

Thomas J. Walters
Equity Trading
(612) 492-8829

Elliott M. Randolph
Institutional Sales Trading
(612) 492-8867

Cory N. Carlson
Institutional Sales Trading
(612) 492-8858

Luke J. Weimerskirch
Institutional Sales Trading
(612) 492-8832

Institutional Sales: (866) 338-3522

Thomas J. Pierce
(612) 492-8817

Mark A. Hagen
(612) 492-8846

Ryan M. Quade
(612) 492-8807

Brandt B. Wendland
(612) 492-8855

John E. Stratton
(612) 492-8826

Jeff R. Sonnek
(612) 492-8825

Matt J. Rasmussen
(612) 492-8860