MobiKEY™

2015 Annual General Meeting November 25, 2015

Legal Notices

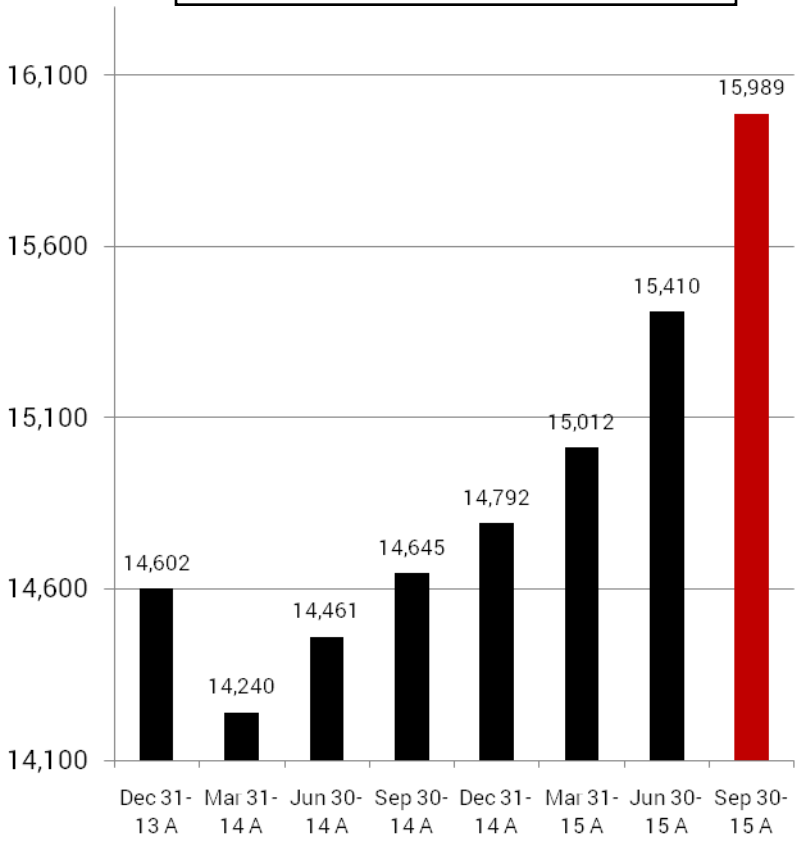
This presentation contains statements that are not current or historical factual statements that may constitute **forward-looking statements**. These statements are based on certain factors and assumptions, including, expected financial performance, business prospects, technological developments, and development activities and like matters. While Route1 Inc. ("Route1" or the "Company") considers these factors and assumptions to be reasonable, based on information currently available, they may prove to be incorrect. These statements involve risks and uncertainties, including but not limited to the risk factors described in reporting documents filed by the Company. Actual results could differ materially from those projected as a result of these risks and should not be relied upon as a prediction of future events. The Company undertakes no obligation to update any forward-looking statement to reflect events or circumstances after the date on which such statement is made, or to reflect the occurrence of unanticipated events, except as required by law. Estimates used in this presentation are from Company sources.

Q3 2015 Highlights

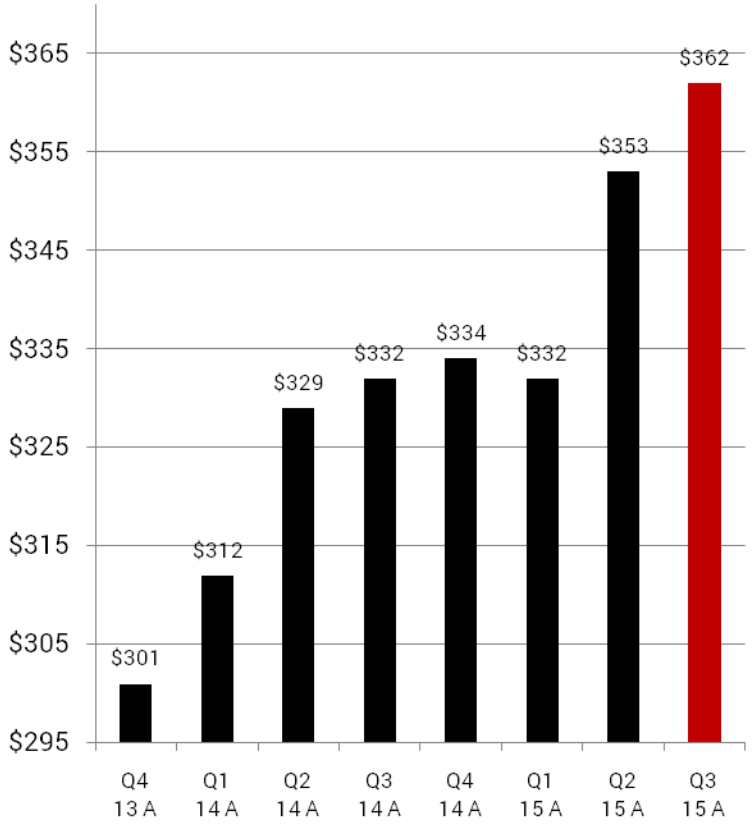
- The June 2015 OPM data breach continues to resonate in Washington
- Small ramp up of our investment in sales and marketing – October 2015
  - Michael Seiler – ex of HPES
  - Enterprise sales rep – lead generation
- MobiKEY 5.0 released in November 2015
- Continued expansion and addition of new US government defense and civilian accounts driving user growth
- The first Route1 blue sky development project is underway – **MobiENCRYPT**

Paid, Active Users

Number of Paid, Active Users



ARPU



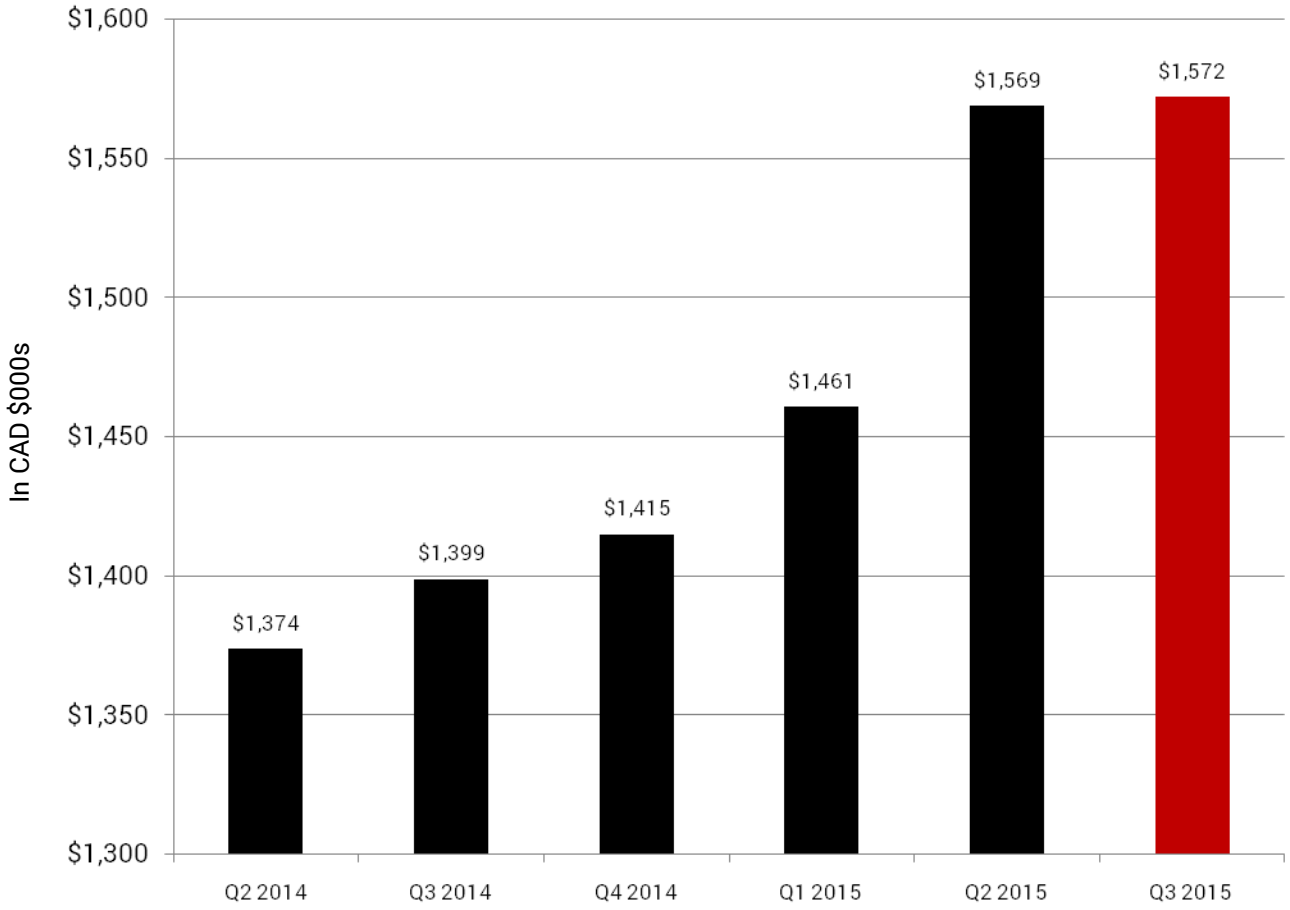
MobiKEY
Securing Enterprise Mobility

Quarterly Operating Performance

In CAD $000s	Q3 A 2015	Q2 A 2015	Q1 A 2015	Q4 A 2014	Q3 A 2014	Q2 A 2014
Revenue	**1,614**	1,620	1,538	1,485	1,432	1,404
Services	1,572	1,569	1,461	1,415	1,399	1,374
Devices, Appliances and Other	42	51	77	70	33	30
Gross Margin	**1,294**	1,326	1,272	1,243	1,110	1,174
Operating Income	**124**	128	314	20	21	26
EBITDA	**242**	227	404	107	110	120
Net Income	**102**	(344)	594	21	210	(34)

MobiKEY™ Securing Enterprise Mobility

Growing Recurring Services Revenue



Note: In the third quarter of 2015, Route1 changed its pricing model for the DON users from a flat fee per month plus a variable fee TO solely a variable fee.

YTD Operating Performance

In CAD $000s	Q3 A 2015	Q3 A 2014	YTD A 2015	YTD A 2014
Revenue	**1,614**	1,432	**4,772**	4,592
Services	1,572	1,399	4,602	4,055
Devices, Appliances and Other	42	33	170	537
Gross Margin	**1,294**	1,110	**3,892**	3,689
Operating Income	**124**	21	**566**	515
EBITDA	**242**	110	**872**	794
Net Income	**102**	210	**351**	616

MobiKEY
Securing Enterprise Mobility

Balance Sheet

In CAD $000s	Sep 30 A 2015	Jun 30 A 2015	Mar 31 A 2015	Dec 31 A 2014	Sep 30 A 2014
Cash	**2,433**	3,468	1,277	1,533	2,601
Total current assets	**3,161**	4,166	3,363	2,246	3,349
Total current liabilities	**3,155**	4,351	2,986	1,926	2,870
Net working capital	**6**	(185)	377	320	479
Fixed and intangible assets	**877**	899	840	563	580
Total assets	**4,466**	5,494	4,631	2,976	4,095
Bank debt	**0**	0	0	0	0
Total liabilities	**3,256**	4,454	3,092	2,031	2,940

MobiKEY
Securing Enterprise Mobility

Quarterly Cash Flow

In CAD $000s	Q3 A 2015	Q2 A 2015	Q1 A 2015	Q4 A 2014	Q3 A 2014
Cash from Operations	**376**	(127)	452	141	298
Change in Working Capital Balance	**(1,249)**	2,749	(312)	(874)	(1,177)
Investing Activities	**(96)**	(158)	(367)	(71)	(29)
Financing Activities	**(66)**	(272)	(29)	(263)	(86)
Cash Inflow(Outflow)	**(1,035)**	2,191	(256)	(1,068)	(994)

MobiKEY
Securing Enterprise Mobility

Securities Outstanding

Security	Number Outstanding
Common Shares	
As at December 31, 2014	**372,773,914**
NCIB Period Purchases	740,000
As at March 31, 2015	**372,033,914**
NCIB Period Purchases	5,668,500
As at June 30, 2015	**366,365,414**
NCIB Period Purchases	1,283,000
As at September 30, 2015	**365,082,414**
NCIB Period Purchases	1,173,000
As at November 15, 2015	**363,909,414**
Stock Options	
As at November 15, 2015	33,964,000

Development Update

MobiKEY
Securing Enterprise Mobility

Competing Factors

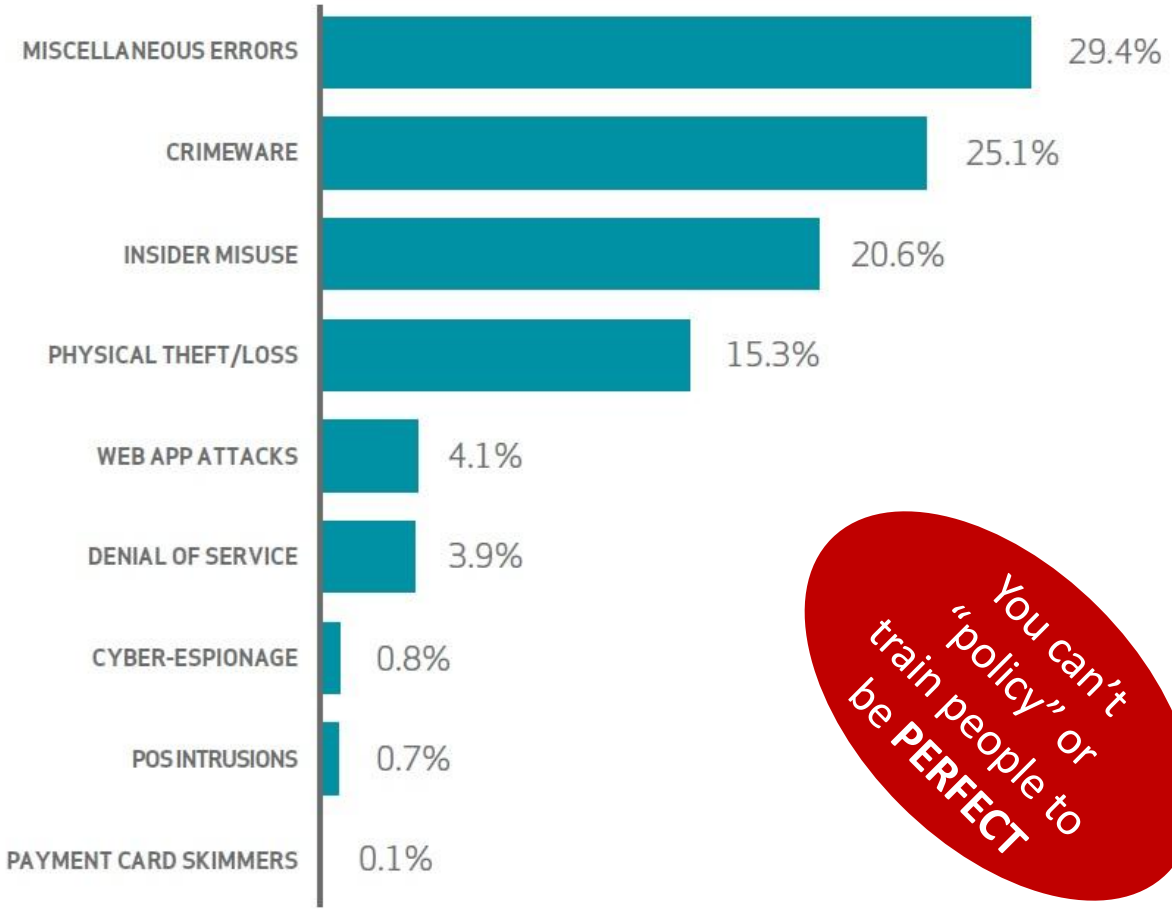
- Employees, remote workers and contractors **demand access** to **their workspace** from anywhere, from any device.
- Unlocking these productivity gains can dramatically increase the **organization's exposure** to security threats and the risk of network breaches. At the same time IT professionals are being asked to support mobility and BYOD initiatives on **tightening budgets**.

MobiKEY
Securing Enterprise Mobility

Data Breach Investigation Report

Verizon 2015 – Data Breach Investigation Report

"It may not be obvious at first glance, but the common denominator across the top four patterns — accounting for nearly 90% of all incidents — is **PEOPLE**. At this point, take your index finger, place it on your chest, and repeat "I am the problem," as long as it takes to believe it."



You can't "policy" or train people to be **PERFECT**

Data Breach Consequences are Growing

- **August 2015: FTC vs. Wyndham Worldwide**
  - US Court of Appeals for the 3rd Circuit handed down its decision in favor of the FTC against Wyndham Worldwide Corporation (Wyndham).
  - This lawsuit was for a failure to implement proper cybersecurity measures and protect consumers' personal information against hackers.
  - The FTC alleged that defendants did not use encryption, firewalls, and other commercially reasonable methods for protecting personal information.
  - What was the basis of the lawsuit?
    - The FTC has started to prosecute companies with inadequate cybersecurity to protect consumer data.
    - In 2008 and 2009 hackers breached Wyndham's network and computer systems 3 separate times.
    - Hackers were able to breach the network due to the **use of weak and obvious passwords**, lack of response to the first incident, and inadequate monitoring systems.
    - The hackers successfully accessed personal information of approximately 619,000 consumers and managed to cause USD $10.6 million in fraudulent charges.
  - What is the effect of the ruling?
    - The ruling affirmed the FTC's authority to bring lawsuits against companies for their lack of cybersecurity measures.

Data Breach Consequences are Growing

- **October 2015**: Enslin vs. The Coca-Cola Company
  - Pennsylvania federal judge has allowed a data breach class action lawsuit against Coca-Cola to proceed.
  - The case is the first case in which a federal court in Pennsylvania allowed a data breach class action to move beyond the motion to dismiss stage.
    - Previous federal courts found other plaintiffs lacked the necessary standing to sue.
  - The case stems from an incident that occurred at the company's distribution center in Atlanta, GA.
    - On Dec. 10, 2013, Coca-Cola discovered that 55 laptops were stolen between 2007 and 2013.
    - The laptops, which were unencrypted, contained the personal information of 74,000 current and former employees of the Coca-Cola Company and six related entities.
    - Social Security numbers, financial information, driver's license information, and other sensitive data were stored on the laptops.
  - In the complaint, Enslin, a former service technician for Coca-Cola, alleged that Coca-Cola did not take the proper steps to protect his information and as a result, his finances were accessed and abused without his authorization.
  - In allowing the case to proceed, U.S. District Judge found Enslin has already suffered palpable harm, including the theft of funds from his bank accounts on two occasions.

What Are We Hearing on the Sales Trail?

- **So long as we meet the appropriate regulatory requirements, i.e. using a VPN, the company is secure.**
- If the technology we are using has a reputable technology brand name, it must be secure.
- If industry peers are using it, it must be secure.
- **My data is not that important so we are good with "okay" security.**
- Data on devices is safe if you have MDM software deployed.
- **I don't know what questions to ask to assess risk with our approach**
- Improved security necessitates a capital investment and increase in *operating* costs.
- The bad guys are smarter than our team; we will be breached at some point in time.

MobiKEY - Access After Authentication

- Smart card based, device independent, 2-factor authentication
- MobiKEY users **do not establish inbound connections**, devices and PCs never become nodes on the enterprise's network
- Users can manipulate files and data but **NEVER REMOVE** from the enterprise's network

MobiKEY Promise

To unlock the productivity gains of enterprise mobility and BYOD without exposing the organization to the risks of data spillage, spyware or malware propagation.

1. High Assurance
   - Meeting the requirements of the most security conscious organizations
2. Plug-and-Play Ease-of-Use
   - End user satisfaction
   - Minimum number of help desk inquiries
3. Enterprise Class
   - Immediately deployable and globally scalable
   - Low total cost of operations (TCO)
   - **Data security is a strategic issue, not an IT issue**

MobiKEY versus a VPN

	MobiKEY	VPN
Multi Factor Authentication	✓ Driven by the identity of the user; smartcard based	X Driven by the software downloaded on the remote PC not the user
Remote Device	✓ Any internet enabled computer can be used safely and securely	X Requires a dedicated and pre-configured remote PC (laptop)
Data Movement	✓ None, all data/files remain behind enterprise firewalls	X Data/files leave enterprise firewalls
Attack Vulnerability	✓ No opportunity for man-in-the-middle, virus, malware	X Susceptible to man-in-the-middle attack, virus, malware
Data Loss	✓ No data is stored on the MobiKEY device. If lost or stolen, can be instantly disabled with one phone call	X Serious security problem if remote PC is lost or stolen. Organization unable to recover data or know who is in possession

MobiKEY versus TeamViewer

	MobiKEY	VPN
Multi Factor Authentication	✓ Strong hardware based authentication driven by the identity of the user - smartcard based. PIV/CAC support.	X Multi-factor authentication optional through available OTP mobile app.
Portability	✓ Any internet enabled computer or mobile device can be used securely. Fully portable - no footprint on remote computer. No endpoint security required.	X Requires installation of client software from the Internet. Risk of phishing attacks. Footprint left-over.
Data Movement	✓ All data/files remain behind enterprise firewalls. No Data at Rest to contend with.	X Permits transfer of data/files beyond enterprise firewalls. High risk of data leakage.
Attack Vulnerability	✓ No opportunity for man-in-the-middle attacks. Mitigates virus and malware vulnerabilities. MobiKEY device inherently trusts only its known Root CAs.	X If the OTP generating app is replicated intruder could potentially impersonate legitimate user. Also, if the endpoint is fooled into using false Public Key of Master, man-in-the-middle attack possible.
Data Loss	✓ No data is stored on the MobiKEY device. If lost or stolen, access can be instantly disabled with one phone call.	X Serious consequences if sensitive data is transferred out. Organization unable to recover data or know who is in possession .

MobiKEY™
Securing Enterprise Mobility

“With MobiKEY, parameters such as what kind of device is requesting access, when was the last OS update, has the latest virus profile been installed, and other device-specific details are not a concern anymore. It just simplifies things tremendously.”

CIO,
Global Insurance Company

MobiKEY
Securing Enterprise Mobility

2015 Business Development Plan

1. Renew key lighthouse accounts.
   - EITSD (the Pentagon)
   - US DHS CBP

2. Build on expanding USG government opportunities.

3. Open up new USG and Canadian government opportunities.
   - The OPM data breach is a strong catalyst for civilian agency growth in 2016

4. Leverage core technological competencies to bring new offerings to market.

MobiKEY 5.0 - A New Baseline

Functionality

Features – Compatibility

- Remote Asset operating system (OS)
  - Android 4.4
  - iOS 6, 7, 8 and 9
  - **Linux Mint, Fedora, Ubuntu or CentOS**
  - Mac OS X 10.7 Lion, 10.8 Mountain Lion, 10.9 Mavericks, 10.10 Yosemite or 10.11 El Capitan
  - Windows XP - 32 bit, Windows Vista – 32/64 bit, and Windows 7, 8.0, 8.1 and 10 - 32/64 bit
- Host Asset OS
  - Windows Vista – 32/64 bit, Windows 7, 8.1 and 10 - 32/64 bit, Windows Server 2008 R2 – 64 bit, and Windows Server 2012 R2 – 64 bit
- Remote audio support for users connecting from Remote Assets running as their OS:
  - Windows Vista – 32/64 bit, and Windows 7, 8.0, 8.1 and 10 - 32/64 bit to a Host Assets with the MobiNET Agent software version 4.4 or higher are installed
  - Mac OS X 10.10 Yosemite or 10.11 El Capitan to a Host Assets with the MobiNET Agent software version 5.0 installed

MobiKEY 5.0 - A New Baseline

Functionality
Features – Usability • Full workspace experience from any device • Turnkey setup and easy integration with existing infrastructure • Plug and play user experience; nothing to install on mobile asset • Cross domain technology; Host Assets can be on any domain or network • Fully integrates with virtual desktop infrastructure (VDI): Citrix and VMWare ready • Integration with Active Directory • Bandwidth efficient - 20 kbps average bandwidth usage per connected user
Features – Administration • HSPD-12 compliant – integrates with CAC or PIV • Internet protocol version 6 (IPv6) support • Connection history details for auditing and reporting purposes • Enterprise registration and deployment tools • Enterprise, group or by user **Policy**

MobiKEY
Securing Enterprise Mobility

MobiKEY 5.0 - A New Baseline

Functionality
Policy • Secure Remote Printing • Secure Remote Scanning • **Bootable MobiKEY** • **Secure Storage** • Password Reset • Host/No Host

MobiKEY Roadmap

Release	Attributes	Timing – On or About
MobiKEY 5.1	Support of multiple smart card readers	Q4 2015
MAP 3.0	Improved UX	Q4 2015
MobiKEY 5.2	New protocol, performance optimizations	Q4 2015 – Q1 2016
MobiKEY for iOS 5.0	Improved UX	Q4 2015
MobiKEY 5.3	Microphone support	Q1 2016
MobiKEY for iOS 5.0 – A2T and TAC support	64 bit support	Q1 2016
MobiKEY for Android 5.0	Improved UX	Q1 2016

MobiENCRYPT

Objective

- To develop a full disk encryption product that can encrypt the Windows operating system partition using the private key in the smart card.

Features

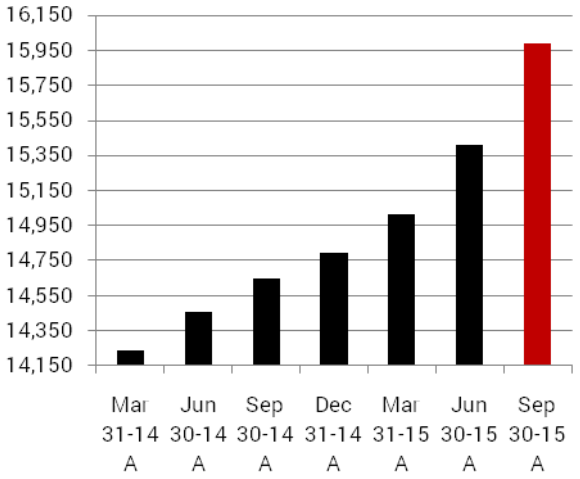
- Transparent Full Disk Encryption: The hard disk will be encrypted/decrypted on-the-fly using AES 256/XTS encryption. This feature will be invisible to most users.
- Pre-boot Authentication: The boot loader will present a text-based interface and will require that a supported device is present and the correct PIN is entered.
- Key Recovery: In addition to the user private key, it will be possible to access the encrypted hard disk using other designated keys.
- Identification of non-encrypted assets: Allow remote queries of MobiENCRYPT status.
- Remote Key Revoke: It will be possible to remotely revoke a user key from the volume encryption keys.

Route1 is on a Path to Market Leadership

- The world's best technology to deliver mobile access for enterprises
- Unlocks mobility without introducing new security risks
- Combines high assurance security with plug-and-play usability
- Current customers include some of world's most security conscious entities like the US DOD
- Positive annual cash flow, net income and debt free
- Growing subscription based revenue model
- Founded in 2004
- 30 employees, 70% in R&D
- LTM repurchased more than 16.7 million shares
- TSX-V: ROI

In CAD $000s	FY 14 Audited	FY 13 Audited
Revenue	**6,078**	5,433
Gross Margin	**4,932**	4,296
Net Income	**637**	(343)

Number of Paid, Active Users



MobiKEY Securing Enterprise Mobility