Route1®

Authentication & Identity Management | Data Security & Secure Communications

Q1 2017 Corporate Update

May 16, 2017

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.

Not for dissemination in the United States or United States newswire services.

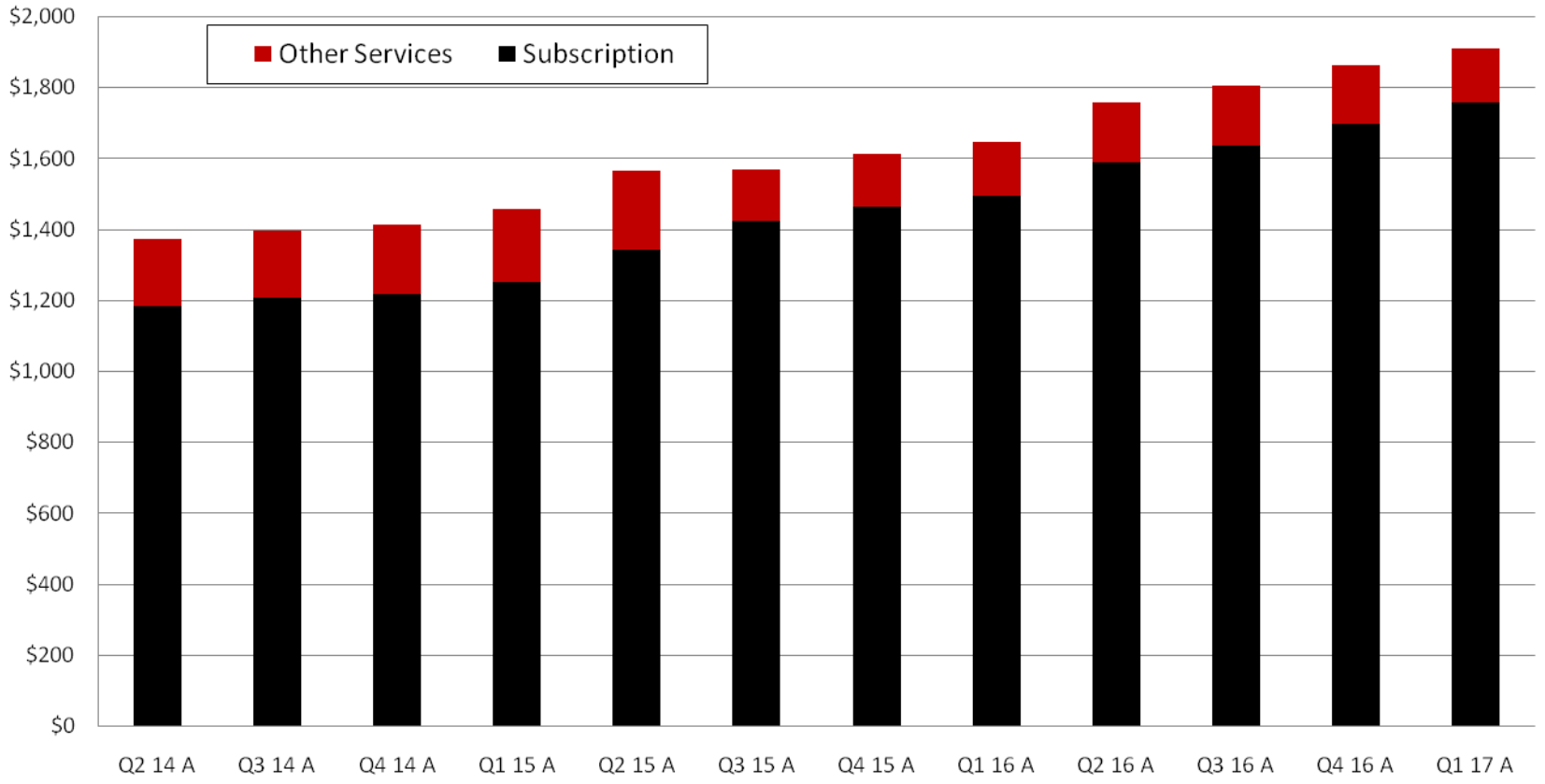
Route1®

Quarterly Operating Performance

In 000s of CAD Dollars	Q1 A 2017	Q4 A 2016	Q3 A 2016	Q2 A 2016	Q1 A 2016	Q4 A 2015	Q3 A 2015	Q2 A 2015
Revenue	**1,941**	1,886	2,031	1,812	1,718	1,625	1,614	1,620
Services	**1,911**	1,865	1,808	1,760	1,648	1,616	1,572	1,569
Devices, Appliances and Other	**30**	21	223	52	70	9	42	51
Gross Margin	**1,606**	1,548	1,583	1,471	1,370	1,341	1,294	1,326
Expenses	**1,289**	1,356	1,243	1,299	1,332	1,189	1,170	1,198
Operating Income	**317**	192	340	172	38	152	124	128
EBITDA	**406**	307	447	278	172	279	242	227
Net Income (Loss)	**208**	91	306	199	(266)	377	102	(344)

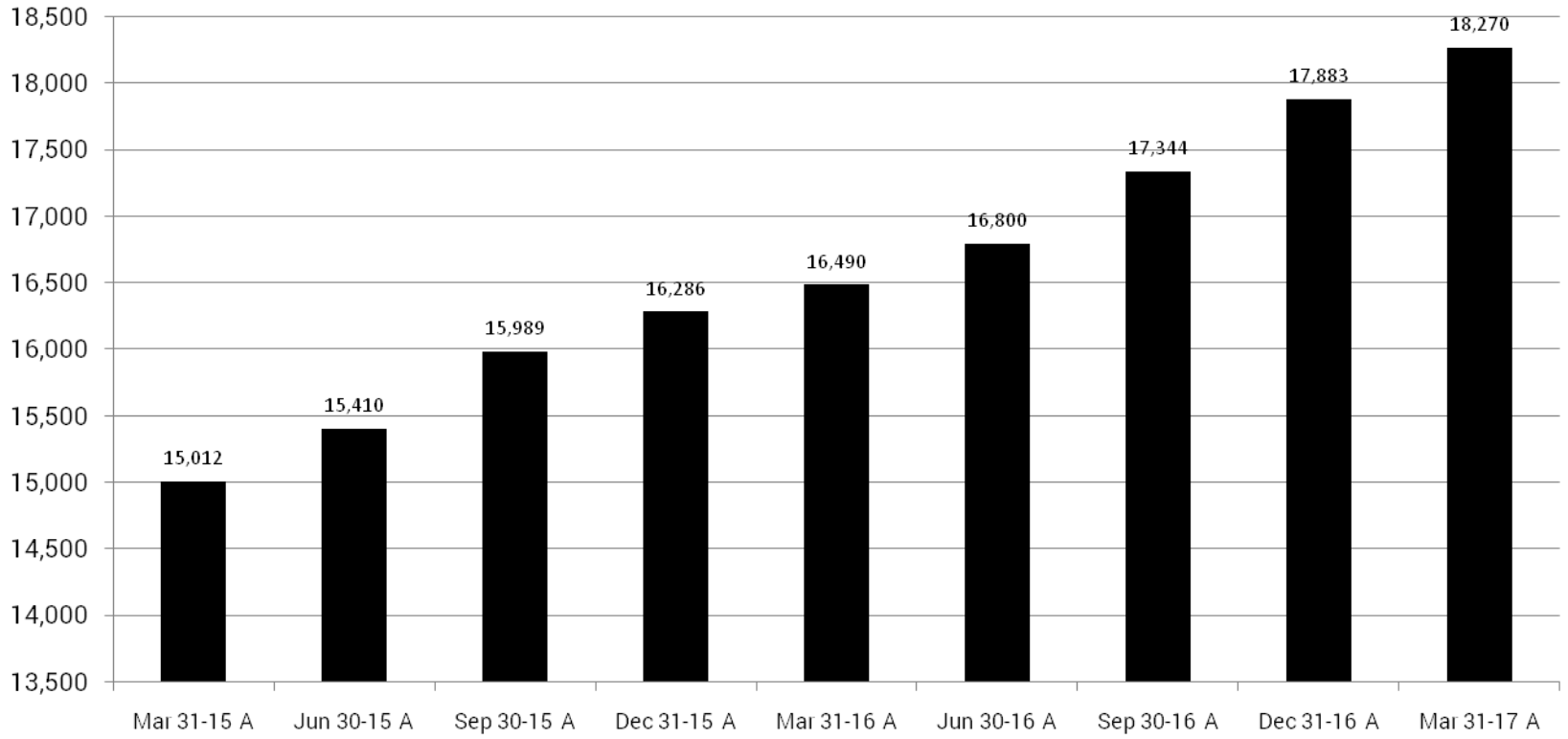
Route1®

Recurring Revenue in CAD 000s



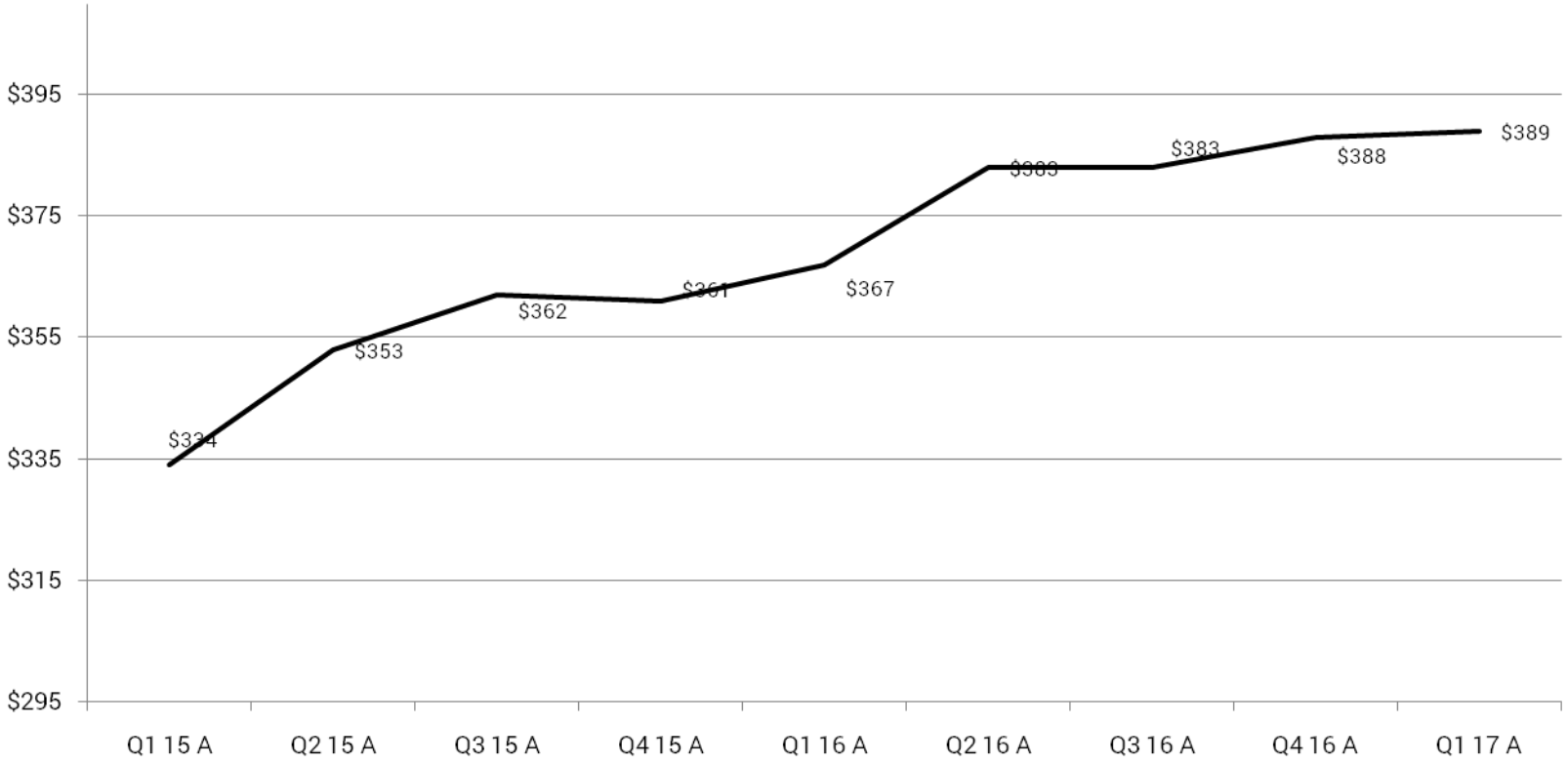
Route1®

MobiKEY Paid, Active Users - No.



Route1®

MobiKEY Paid, Active Users - ARPU



Route1®

Balance Sheet

In 000s of CAD Dollars	Mar 31 2017 A	Dec 31 2016 A	Sep 30 2016 A	Jun 30 2016 A	Mar 31 2016 A	Dec 31 2015 A
Cash	**704**	1,946	2,898	3,735	407	1,251
Total current assets	**1,890**	2,910	3,938	4,765	3,880	2,112
Total current liabilities	**1,113**	2,500	3,555	4,719	3,814	1,948
Deferred revenue (included in current liabilities)	**777**	2,155	3,312	4,506	3,531	1,657
Net working capital	**777**	410	383	46	66	164
Fixed and intangible assets	**481**	537	550	609	674	801
Total assets	**3,114**	4,190	5,230	6,116	5,296	3,656
Bank debt	**0**	0	0	0	0	0
Total liabilities	**1,210**	2,590	3,656	4,820	3,919	2,059
Shareholders' Equity	**1,904**	1,600	1,574	1,296	1,377	1,597

Route1®

2017 Plan

Initiative	Outcome	Driver
1. **IP Realization**	• Payment/license • Sale of the IP • Strategic sales arrangement	• Infringement lawsuit against VMware/AirWatch
2. **MobiKEY Organic Growth**	• Expect material growth in MobiKEY users	• DoD accounts • New account groups
3. **Match Expense to Revenue Profile**	• Cash flow positive, and growing	• Loss of CBP MobiKEY account
4. **Merger or Acquisition**	• Deal dependent	• Technology, client vertical diversification • Critical mass
5. **New Sales – DerivID**	• Sales in 2018 and beyond	• Derived credential push by DISA and NIST
6. **New Technology** – Universal Method for Authenticating a User	• Introduction and sales in 2018	• Market assessment • Consumer, SME

Last 30 Days in Washington

- Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure issued May 11, 2017
  - In alignment with our current MobiKEY messaging, security first architecture, no data at rest, no data in transit, not vulnerable to man-in-the-middle attacks, while using PIV/CAC-based authentication
  - Elevating the accountability for managing cybersecurity risk beyond the CIO and CISO levels to the heads of the executive departments and agencies; we believe this move is positive as it moves the cybersecurity discussion beyond an IT discussion
  - Agency heads are directed to use the Framework for Improving Critical Infrastructure Cybersecurity developed by NIST
  - Agency heads are advised to show preference in their procurement for shared IT services, including email, cloud, and cybersecurity
  - With the short deadline for all of the initial reports, the creation of these initial reports will now become the short-term focus of the government
  - There is an entire section dedicated of the Executive Order dedicated to critical infrastructure

Last 30 Days in Washington

- Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure issued May 11, 2017
  1. Identification of risks in a consolidated report per department and elevation of accountability and responsibility to heads of departments and agencies are ***positive changes which will result in increased attention to cybersecurity***
  2. Moving towards shared IT services and converged technologies are expected to lead to government being more agile and recognizing cost savings, although ***it is imperative that this isn't done at the expense of cybersecurity***
  3. As a cybersecurity technology provider to the government, we believe the Executive Order is ***a step in the right direction and presents both opportunity and risk as the government lays the groundwork to move towards shared IT services***

- Budget approved May 4, 2017, providing funding through the end of the current fiscal year (September 30, 2017)
  – Certain Federal opportunities we are working on wouldn't purchase until there was an approved budget in place; working to advance those initiatives

Connecting with the Marketplace

Target Markets

- U.S. Government – DOD and Federal (civilian) focused
- Canadian Government on an opportunistic basis
  - Attended a NATO conference at the end of April to expand our government focus beyond North America
- Certain segments of the enterprise vertical are responsive to our messaging: critical infrastructure, financial services, professional services, healthcare and SMBs

Promotion

- Direct sales supported by client conferences and industry/vendor events
  - High value placed on relationships with decision makers
- Leveraging Route1 Board members, strategic partners and resellers to assist in warm introductions to key decision makers
- Invested in a sales intelligence tool, to assist is shortening the prospecting cycle for non-government initiatives in Canada
- Using social media to push broader market themes; opportunistic commentary based on market events, i.e. data breaches

Vulnerabilities Being Exploited by WannaCry

- WannaCry is a ransomware program targeting the Microsoft Windows operating system
- On May 12, 2017 a large cyber-attack was launched using it, infecting more than 230,000 computers in 150 countries, demanding ransom payments
- The attack spreads by phishing emails, but also uses an exploit published in WikiLeaks - Vault 7
  - A "critical" patch had been issued by Microsoft on March 14, 2017 to remove the underlying vulnerability for supported systems, but many organizations had not yet applied it
  - Those still running exposed older, unsupported operating systems were initially at particular risk, but Microsoft has now taken the unusual step of releasing updates for these
- SMB and potentially RDP are a means used by the virus to propagate *horizontally* within a network
- **The principal reasons MobiKEY is not vulnerable to this type of exploit are because it doesn't require any inbound ports to be open and all communications are mutually authenticated**

Business Development Update

- Joint Service Provider renewed their MobiKEY enterprise subscription at the end of March 2017
  - The contract is for the base year plus two option years, we have received full payment for this renewal
- We continue to see month over month growth with the Department of the Navy and we continue to focus business development efforts to grow and expand this account
- Navy Bureau of Medicine and Surgery has expanded their use of the MobiKEY technology to additional geographic locations
- The critical infrastructure vertical is taking cybersecurity more seriously and our MobiKEY messaging is starting to resonate
- The loss of US Customs and Border Protection is isolated to them and has not had a spill over effect to other US government customers

Using MobiKEY for a Different Use Case

"Tweak" our current MobiKEY technology for use cases in different verticals

For example, the industrial automation application: Provide real-time data collection from Programmable Logic Controllers (PLCs), data analytics, and quantitative-based recommendations to minimize downtime, drive efficiency and minimize cost: architected to ensure that the approach is secure, easily deployable, and scalable

- A PLC is a digital computer used for industrial automation processes, such as control of machinery on factory assembly lines, packaging, food, amusement parks, light fixtures, wind farms, smart parking garages, etc.
- Sensors provide real-time data to the PLC so that the PLC can determine when it can advance to the next stage of the process.
  - It is the intelligent analysis of this data that will lead to identification of automation issues, opportunities for improvement, re-engineering requirements, cost reduction, increases in production, etc.

MobiKEY Development

Release	Attributes	Timing
MobiKEY for Android 5.1 – Soft App and A2T	• Support for Android 5.x and 6.x • Knox support	Released - April 2017
MobiKEY 5.2	• An updated version of the remote control mechanism using a new version of our protocol (v2) is now supported • Multiple monitors on the Remote Asset are now supported; users will have the option to use additional monitors to fully utilize the Remote Assets hardware capabilities • Improved screen size and resolution negotiation between Remote and Host Assets • Remote Assets running Mac OS Sierra (version 10.12) are now supported • Bidirectional audio will be supported • Improved security for Host Assets while in a data session • Performance optimizations • Miscellaneous bug fixes	May 2017
DerivID 1.1	• iOS support	June 2017

Route1®

Surfacing the Value Embedded in our IP

Specific Patent Infringement – the 216 Patent

- Commenced analysis of possible infringement by AirWatch in Q2 2016
- AirWatch is a wholly-owned subsidiary of VMware, Inc. (NYSE: VMW)
- Retained counsel in fall 2106 to provide legal analysis of infringement
- Analysis completed in early 2017
- Entered into hybrid fee arrangement with patent litigation counsel - Vorys, Sater , Seymour and Pease LLP
  - Legal services provided at discount to normal rates in return for a participation in the award/recovery
  - Route1 will pay third party costs
- Filed complaint against AirWatch in Delaware court March 27, 2017 – will serve before June 25, 2017
- **Route1 has the financial capacity to see the complaint through trial based on cash on hand and expected future cash flow generated by operations**

U.S. Patent No. 7,814,216

- Route1's U.S. Patent No. 7,814,216 (216 Patent), "System And Method For Accessing Host Computer Via Remote Computer", was issued by the United States Patent and Trademark Office on October 12, 2010 and expires on March 3, 2025
  - Route1 is the owner by assignment of the entire right, title and interest in the 216 patent, including the sole and undivided right to sue for infringement
- The 216 Patent is generally directed to using a controller to enable secure communication between a remote device, such as a smartphone or a portable computer, and a host computer
  - The controller, remote and host are in different locations; the host is usually part of a customer's computer system
- **Route1 believes this patent is an important patent to the broader EMM and MDM vertical**

Surfacing the Value Embedded in our IP

- Reached out to VMware and other parties that we believe have an interest in talking to us about our 216 Patent and more broadly, Route1's intellectual property (patent portfolio)
  - The AirWatch complaint initiation is the first step in the process

- Having commercial discussions to see where they take us re **actualizing on the value of our IP**

- Not excluding potential options at this point in time

Capital Markets Commentary

- Largest shareholder - Fiera - held 45,519,360 shares (12.97%) of ROI in funds it managed
  - Sold entire position from April 24 to April 28, 2017; ROI had no communication with Fiera during that period
  - Based on available information, a number of buyers purchased the block over several days

- Pursuant to the NCIB, ROI purchased 1,000,000 shares at $0.015

The Next 90 Days

1. Actively pursue actualization of the value of our IP

2. Serve our complaint against AirWatch and proceed with the litigation

3. Increase the number of MobiKEY users within core DoD accounts

4. Push our messages with the key US government stakeholders based on the content of the Cybersecurity Executive Order

5. Close on “first” MobiKEY opportunities with critical infrastructure vertical

6. Finalize our plan for a new application or use case for MobiKEY – as an example, the industrial automation vertical

Route1®

Authentication & Identity Management | Data Security & Secure Communications

Q1 2017 Corporate Update

May 16, 2017