

Client: New York Strategy

Physical Address:

457 Madison Ave
New York, NY 10022

Data Management, Inc.
3322 West Loop 306
San Angelo, TX 76904



CREDIT CARD AUTHORIZATION

Please print out this form, fill out completely, and return fax to Data Management at (325) 223-9104.

Company: Little St. James, LLC Credit Card Billing Address: Little St. James, LLC
600 RED HOOK QTR
B-3
St. Thomas USVI
00802

Cardholder Name: JEFFREY EPSTEIN

Phone Number: [REDACTED]

Please forward this form to my sales representative promptly. Representative name: [REDACTED]

I, JEFFREY E. EPSTEIN, give Data Management, Inc permission to charge the amount of \$ 1054.20, for this purchase (including any shipping and taxes) to the credit card below.

Please keep this credit card number and authorization on file for any future purchases. (Check One)

- Yes. Please consider this single form to be authorization for all future purchases.
- No. I will fill out an authorization form each time I make a credit card purchase.

Please check one:

VISA MASTERCARD AMERICAN EXPRESS DISCOVER

Credit Card Number: [REDACTED] Expiration Date: 05/10

Name on Credit Card: JEFFREY EPSTEIN

Signature: [Handwritten Signature]

Date: 7/25/07

This document is confidential and shall not be duplicated, published or disclosed, in whole or in part, without prior written permission of Data Management, Inc. The terms and conditions herein are subject to change without notice.

TimeClock Plus™
 by Data Management, Inc.
 3322 West Loop 306, San Angelo, TX 76904
 [Redacted] fax: [Redacted]
 [Redacted]@timeclockplus.com

Invoice No.	Customer#	Order Date
224584	129519	04/20/2007

SOLD TO
New York Strategy Emad Hanna 457 Madison Ave New York, NY 10022

SHIP TO
New York Strategy Jermane Ruan Little St. James Island 6100 Red Hook Quarters B-3 Saint Thomas, VI 00802

Rep	Entry	Method of Shipment	Method of Payment
MMURCHISON	JAMES	Fed-Ex Customer	American Express [Redacted] Exp 02/2009

Stock No.	Ordered	Shipped	Description	Unit Cost	Total
10-10	1		Money Back Guarantee Waiver	0.00	0.00
40-193	1		Mark III Waterproof Clock Enclosure	519.00	519.00
			Fed-Ex Customer Overnight		

Customer Invoice
 This is the ONLY invoice you will receive



Subtotal: 519.00
 S & H: 9.00
 Tax: 0.00
 Total: 528.00

TimeClock Plus™
 by Data Management, Inc.
 3322 West Loop 306, San Angelo, TX 76904
 fax: [REDACTED]
 [REDACTED]@timeclockplus.com

Quote No.	Customer#	Quote Date
107296	129519	04/18/2007

CUSTOMER
New York Strategy Emad 457 Madison Ave New York, NY 10022

Rep	Entry	Method of Shipment	Method of Payment
MMURCHISON	MMURCHISON	N/A	Pre-Paid

Stock No.	Ordered	Description	Unit Cost	Total
20-402	1	TimeClock Plus Professional Edition	2,190.00	2,190.00
	50	Professional Ed Employee Licenses		
	10	Professional Ed User Licenses		
		TimeClock Plus Professional Edition Discount	-400.00	-400.00
30-366	1	QuickBooks Pro Payroll (Export Module)	270.00	270.00
41-204	1	BIO RT+ Serial Pin Punch	3,225.00	3,225.00
		Wi-Fi 802.11b Network Interface for RT Series		
		BIO RT+ Serial Pin Punch Discount	-400.00	-400.00
43-817	1	UPS Battery Module	185.00	185.00
40-193	1	Mark III Waterproof Clock Enclosure	519.00	519.00

Valid for 60 days. Expires 04/24/2007.
 DO NOT PAY. THIS IS NOT AN INVOICE.



Emad approved By *JF*
 4/20/07

Subtotal: 5,589.00
 S & H: 9.00
 Tax: 0.00
 Total: 5,598.00

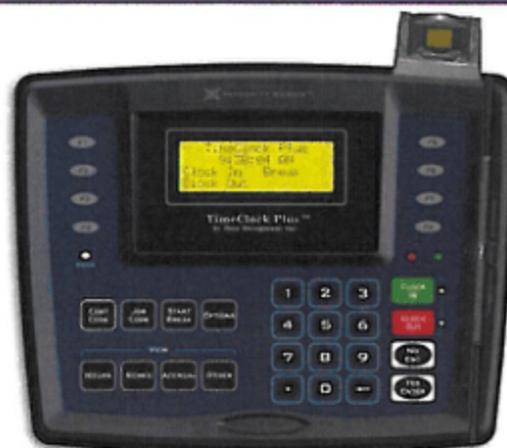
Money back guarantee: if applicable, begins on date of shipment.
 Money back guarantee does not apply to S&H, encoded or printed badges, specially order items, or lease purchases. Visit www.timeclockplus.com dm: guarterms.asp

Product Line: Integrity Series

TimeClock Plus Finger Biometric Terminal

Sensor Specifications:

- Silicon Capacitor Sensor
- Operating Temperature: 32 - 120 F (0 to 55 C)
- Allowable Finger Rotation: 360 degrees
- Max Internal Prints: 1300
- Sensor LED's: Green = Successful, Red = Failure, Amber = Waiting for scan



Software Required: TimeClock Plus 5.0

Hardware Supported: Xipher Integrity Series RT/RT+

Fallback Mode Support: Yes

Internal Prints stored in Sensor: 1300

Internal Punches stored in Fallback Mode: 2000

Reader Support: Magnetic, Bar Code, Proximity

Enrollment: You can enroll up to 5 prints per employee. During enrollment, the template (print) is stored internally in the sensor as well as in the TimeClock Plus database. After enrollment, you can synchronize the templates between a reader and the database. This prevents you from having to enroll at each terminal, you enroll at a central terminal, and then synchronize templates with the database at the other terminals.

Template Synchronization: You can synchronize templates with the readers and the database. If a template for an employee is not found in the internal sensor flash during a clock operation and there is a template for the employee in the database, it is uploaded to the internal sensor flash to verify against before the clock operation.

Security Concerns: A problem with traditional optical sensors is that they can be 'fooled' by copy images of a fingerprint, such as with molds, etc. With silicon sensors, the fingerprint is much more difficult to be 'fooled'. This is because the silicon sensors does not take a traditional picture of the print as with optical sensors, but generates the image by measuring the electrical conductivity of the fingerprint using the ridges and valleys of the fingerprint. Because of this, it cannot be as easily duplicated by a copy or finger mold.

Release: 5/1/06

TimeClock Plus Finger Biometric Reader Product Brief

TimeClock Plus Xipher Integrity Series Wireless Terminal Configuration

Note: The Xipher Integrity Series Wireless Terminal supports the 802.11b wireless standard. The 802.11b wireless standard operates on the 2.4 GHz frequency, which can be susceptible to interference from other wireless devices operating on the 2.4 GHz frequency as well. An example would be a cordless phone operating on the 2.4 GHz frequency. Interference from other devices operating on the 2.4 GHz frequency can cause loss of communication to the Xipher Terminal, if this occurs, you may try changing the channel that your other wireless device operates on to reduce the interference.

Entering the Configuration for the Wireless Terminal:

To enter the Integrity Series Setup, press and hold the **F1** key and the **Yes/Enter** key, at the same time, within 5 seconds of supplying power to the terminal. This will enter the Integrity Series Setup. If the Ethernet terminal shows "Waiting for Host" once you have connected it to the power supply, then simply reset the power and press and hold the **F1** and **Yes/Enter** keys, at the same time, within 5 seconds of recycling the power.

Configuring the Network Settings:

1. The Integrity Series Terminal will prompt you for "Checkout?". Press the **NO** button. Checkout Mode is an offline diagnostic program and is not necessary to run at this time.
2. The Integrity Series Terminal will prompt you for "Setup?". Press the **YES** button.
3. The Integrity Series Terminal will prompt you for "Network Settings?". Press the **Yes** button.
4. The screen will show the current IP Address configuration for your Ethernet Terminal. If you are unfamiliar with IP address, please contact your network administrator. Enter the four numbers representing your IP address. This IP address must be accessible by the PC / Server that will be running the WinRemote application.
5. Once you have entered the IP address, Press the **Enter** button. Once the IP address is entered, the Integrity Series Terminal will prompt for a Subnet Mask, so you should enter your network Subnet Mask. If you are not familiar with your network Subnet Mask, please contact your network administrator.
Note: If you make a mistake, you can press the **No\Esc** key to reset the IP Address.
6. Once you have entered the Subnet Mask, Press the **Enter** button. Once the Subnet Mask is entered, the Integrity Series Terminal will prompt for a Default Gateway, so you should enter your networks Default Gateway. If you are not familiar with your networks Default Gateway, please contact your network administrator.
Note: If you make a mistake, you can press the **No\Esc** key to reset the Subnet Mask or Gateway.
7. Once you have entered the Default Gateway, Press the **Enter** button. Once the Default Gateway is entered, the Integrity Series Terminal will prompt for a Local Port. The Local Port address is set to a default of 3001. This setting should be left at the default of 3001 unless instructed to change it by a TimeClock Plus Support Technician.

Configuring the SSID (Service Set Identifier)

8. Press the **Enter** button after configuring the Terminal Port number to cycle through all other network settings until you come to the screen that prompts you for "SSID:". At this screen you can enter the SSID. The SSID can include Alphanumeric characters (A-Z) and Numeric characters (0-9).

XIPHER WIRELESS TERMINAL INSTALLATION GUIDE

To enter the SSID, the following keys can be used to specify the characters and numbers:

- The HOURS button allows you to enter upper case characters, beginning at 'M'. You may press the Clock In and Clock Out keys to cycle through the list of upper case characters. Once the correct character is specified, press the period key '.' to accept that character.
- The SCHED button allows you to enter lower case characters, beginning at 'm'. You may press the Clock In and Clock Out keys to cycle through the list of lower case characters. Once the correct character is specified, press the period key '.' to accept that character.
- The ACCRUAL button allows you to enter numbers, beginning at '5'. You may press the Clock In and Clock Out keys to cycle through the list of numbers. Once the correct number is specified, press the period key '.' to accept that character.

***Note:** You can use the '←' key to delete previously entered characters or numbers. The period '.' advances to the next character.

Once you have the entire SSID entered, press the **Enter** key to continue.

Configuring the Security Settings for WEP (Wired Equivalent Privacy) Security

1. If you have WEP Security enabled on your network, follow these steps to configure the Wireless Terminal with your WEP Security options. If you have WPA Security enabled on your network, please refer to the next section for the steps on Configuring the Security Settings for WPA Security.

***Note:** If you are not familiar with your security settings enabled on your wireless network, please consult your IT Department or Network Administrator for the security settings (WEP, WPA, Encryption, or Passphrase Keys).

2. To Enable WEP Security, after entering the SSID, the next screen is Security. You can cycle through the security options by pressing the Clock In and Clock Out keys. The options include None, WEP, or WPA. Set the Security to WEP and press the **Yes/Enter** key.
3. The next screen will prompt you for Encryption. You can cycle through the encryption options by pressing the Clock In and Clock Out keys. The available Encryption settings are 64 bit or 128 bit encryption. Specify the level of encryption that you have configured for WEP Security on your wireless network and press the **Yes/Enter** key to accept the value.
4. Once you specify either 64 bit or 128 bit encryption, you will be prompted to enter the Encryption Key. The encryption key can be Hexadecimal, meaning it can range from 0-9, A-F. To specify the key, you can cycle through the available characters by pressing the Clock In or Clock Out keys. Once you have a character set, press the period key '.' to accept that character. Once you have entered the entire encryption key, press the **Yes/Enter** key to save the key.
5. The Integrity Series Terminal will prompt you for "Aux Settings?". Press the No/Esc button to bypass these settings.
6. The Integrity Series Terminal will prompt you for "Reader Settings?". Press the No/Esc button to bypass these settings.
7. The Integrity Series Terminal will prompt you to "Exit?". Press the **Yes/Enter** button to exit the Network Setup and you are then prompted to "Save Changes?". Press the **Yes/Enter** button to save the changes that were made.
8. The Integrity Series Terminal will prompt you to "Exit?". Press the **Yes/Enter** button to exit the offline setup mode and reset the unit so that it can accept communication from the software.

***Note:** You can use the '←' key to delete previously entered characters or numbers. The period '.' advances to the next character.

© Data Management, Inc. 2005. All Rights Reserved. This document is confidential and shall not be duplicated, published or disclosed, in whole or in part, without prior written permission of Data Management, Inc. This documentation is subject to change without notice.

Configuring the Security Settings for WPA (WiFi Protected Access) Security

1. If you have WPA Security enabled on your network, follow these steps to configure the Wireless Terminal with your WPA Security options. If you have WEP Security enabled on your network, please refer to the next section for the steps on Configuring the Security Settings for WEP Security.

***Note:** If you are not familiar with your security settings enabled on your wireless network, please consult your IT Department or Network Administrator for the security settings (WEP, WPA, Encryption, or Passphrase Keys).

2. To Enable WPA Security, after entering the SSID, the next screen is Security. You can cycle through the security options by pressing the Clock In and Clock Out keys. The options include None, WEP, or WPA. Set the Security to WPA and press the **Yes/Enter** key.
3. The next screen will prompt you for Key Type. You can cycle through the Key Type options by pressing the Clock In and Clock Out keys. The available Key Type settings are Hex Key or Passphrase. Specify the type of Key that you have configured for WPA Security on your wireless network and press the **Yes/Enter** key to accept the value.
 - If you specify Hex Key, you will be prompted to enter the Hex Key. The Hex key can be Hexadecimal, meaning it can range from 0-9, A-F. To specify the Hex key, you can cycle through the available characters by pressing the Clock In or Clock Out keys. Once you have a character set, press the period key '.' to accept that character.

Once you have entered the entire Hex Key, press the **Yes/Enter** key to save the Hex Key entered.

- If you specify Passphrase, you will be prompted to enter the Passphrase. The Passphrase can include Alphanumeric characters (A-Z) and Numeric characters (0-9).

To enter the Passphrase, the following keys can be used to specify the characters and numbers:

- The HOURS button allows you to enter upper case characters, beginning at 'M'. You may press the Clock In and Clock Out keys to cycle through the list of upper case characters. Once the correct character is specified, press the period key '.' to accept that character.
- The SCHED button allows you to enter lower case characters, beginning at 'm'. You may press the Clock In and Clock Out keys to cycle through the list of lower case characters.

Once the correct character is specified, press the period key '.' to accept that character.

- The ACCRUAL button allows you to enter numbers, beginning at '5'. You may press the Clock In and Clock Out keys to cycle through the list of numbers. Once the correct number is specified, press the period key '.' to accept that character.

***Note:** You can use the '<' key to delete previously entered characters or numbers. The period '.' advances to the next character.

4. Once you have the entire Passphrase entered, press the **Enter** key to continue.

© Data Management, Inc. 2005. All Rights Reserved. This document is confidential and shall not be duplicated, published or disclosed, in whole or in part, without prior written permission of Data Management, Inc. This documentation is subject to change without notice.

XIPHER WIRELESS TERMINAL INSTALLATION GUIDE

5. The Integrity Series Terminal will prompt you for "Aux Settings?". Press the No/Esc button to bypass these settings.
6. The Integrity Series Terminal will prompt you for "Reader Settings?". Press the No/Esc button to bypass these settings.

7. The Integrity Series Terminal will prompt you to "Exit?". Press the **Yes/Enter** button to exit the Network Setup and you are then prompted to "Save Changes?". Press the **Yes/Enter** button to save the changes that were made.
8. The Integrity Series Terminal will prompt you to "Exit?". Press the **Yes/Enter** button to exit the offline setup mode and reset the unit so that it can connect to your wireless access point and begin accepting communication from the software.

Data Management, Inc.
3322 West Loop 306
San Angelo, TX 76904



CREDIT CARD AUTHORIZATION

Please print out this form, fill it out, and return fax to DMI at [REDACTED], to the attn of Melanie Murchison.

Card Holder Billing Information:

Company:
New York Strategy

(This address must match billing statement)

Credit Card Billing Address:
457 Madison Ave

Phone Number:

City: New York St: NY Zip: 10022

[REDACTED]
(###) ###-####

Terms of Purchase: (Please Print Clearly)

I, Jeffrey Epstein, give Data Management, Inc permission to charge the amount of \$ 528.00 for this purchase (including any applicable shipping and taxes) to the credit card below. I also authorize, only if selected below, Data Management, Inc. to charge this card for future purchases originated by myself or others at this Company.

Please keep this credit card number and authorization on file for any future purchases. (Check One Please)

- Please consider this single form to be authorization for all future purchases
- I will fill out an authorization form each time I make a credit card purchase from DMI.

Credit Card Information:

Please check one:

- VISA
- MASTERCARD
- AMERICAN EXPRESS
- DISCOVER

For security purposes, when faxing or emailing, at your discretion, feel free to leave the Credit Card number field blank, and telephone your sales representative directly to provide the CC number for processing.

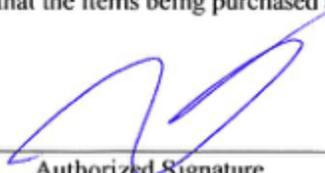
Credit Card Number: [REDACTED]
(XXXX-XXXX-XXXX-XXXX)

Expiration Date: 02-09
(MM-YY)

Name as it appears on Credit Card: Jeffrey Epstein

Signature of Authorized Purchaser:

I understand that the items being purchased are not eligible for DMI's Money Back Guarantee and are non-refundable.



Authorized Signature

04.20.2007
Date

Data Management, Inc.
3322 West Loop 306
San Angelo, TX 76904



CREDIT CARD AUTHORIZATION

Please print out this form, fill it out, and return fax to DMI at [REDACTED] to the attn of Melanie Murchison.

Card Holder Billing Information:

Company:
New York Strategy

(This address must match billing statement)

Credit Card Billing Address:
457 Madison Ave

Phone Number:

City: New York St: NY Zip: 10022

[REDACTED]
(###) ###-####

Terms of Purchase: (Please Print Clearly)

I, Jeffrey Epstein, give Data Management, Inc permission to charge the amount of \$ 5029.00 for this purchase (including any applicable shipping and taxes) to the credit card below. I also authorize, only if selected below, Data Management, Inc. to charge this card for future purchases originated by myself or others at this Company.

Please keep this credit card number and authorization on file for any future purchases. (Check One Please)

- Please consider this single form to be authorization for all future purchases
- I will fill out an authorization form each time I make a credit card purchase from DMI.

Credit Card Information:

Please check one:

- VISA MASTERCARD AMERICAN EXPRESS DISCOVER

For security purposes, when faxing or emailing, at your discretion, feel free to leave the Credit Card number field blank, and telephone your sales representative directly to provide the CC number for processing.

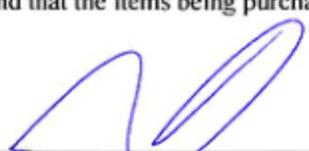
Credit Card Number: [REDACTED]
(XXXX-XXXX-XXXX-XXXX)

Expiration Date: 02-09
(MM-YY)

Name as it appears on Credit Card: Jeffrey Epstein

Signature of Authorized Purchaser:

I understand that the items being purchased are not eligible for DMI's Money Back Guarantee and are non-refundable.



Authorized Signature

04.20.2007
Date