# User's Guide
# Rossware's Virtual CC Terminal
# (Rev. 1.0.3)

This utility was first created in December of '08. It allows you to process credit card transactions from within ServiceDesk, SD-Mobile or SD-RevenueBuilder. It may also be used as a stand-alone utility, without integration to any other Rossware products.

As you'll see upon trying it, our Virtual Terminal allows you to either *type-in* the applicable credit card data, or to *swipe* the customer's credit card through a computer-attached MCR (magnetic card reader, aka "swiper") device. Where possible, the latter method is preferred, because the resulting merchant fees are lower (of course, swiping also eliminates the labor of manual entry).

We have programmed the utility to work with just one credit card processing company, and for a very good reason. Every processing entity has significant differences in how a "terminal" must connect and communicate to carry off a transaction. If we were to make our terminal adaptive to all such variations, we'd be forced to manage enormous complexity in such regard. Instead, we've kept it very simple—both for us (in terms of programming), and for you (in terms of setup).

## *Chapter 1*

### Setting Up Your Merchant Gateway

The processing company we've selected is Cayan (formerly Merchant Warehouse). We chose this company because of its integrity. Under the arrangements we have with Cayan, it is imposing zero setup cost, and no contract. That says a lot. It says, in short, the only way they're going to make money is by keeping you happy.

They also guarantee to meet or beat whatever rates you are paying with your present processor (unless you already have "stinking good" rates, you can pretty much count on the fact they'll be offering significantly better ones). Depending on your volume, they may also offer to waive any monthly service fee.

To setup your Cayan account, please begin (assuming you've not yet done so) by contacting us here at Rossware. Just let us know you're ready. We'll initiate the process for you. We need to do this so that: (a) you receive the special terms available via our arrangement; and (b) your account is properly setup to work with our Virtual Terminal.

Within a short time, you'll be contacted by a Cayan representative, who will shepherd you through the easy application process.

By the way, you're going to find the folks there want to review a couple months of prior statements from your existing processor (assuming, of course, you have one). Please don't let this bother you. Every merchant processor does this. It's actually beneficial to you, as it allows them to understand what your transaction patterns are, the better to tailor an optimum account setup on your behalf.

# *Chapter 2*

## Installing the Program

If you're using Virtual Terminal as an embedded feature within another Rossware product, there's nothing to install (it's already in the other product), and you may skip this section.

If you're using it is a stand-alone product, simply place the install CD into your computer's CD drive. When the auto-menu appears, choose *Install Program*.

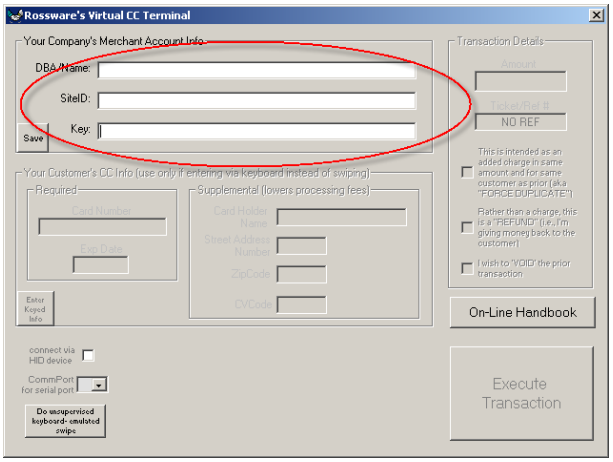
There will be a few prompts during the install. You *could* look for and carefully choose the appropriate button to click in each instance—but that would be an unnecessary effort (something we don't like). If instead you just *Enter* on your keyboard at each query, you'll be fine (it's what we recommend).

Once the install is complete, click on your Windows *Start* button, choose *Programs*, then *Rossware Computing*, and you'll find *Virtual Terminal* after that. Click to run, and you're on your way.

# *Chapter 3*

## Entering Your Merchant Credentials in the Virtual Terminal

When Cayan creates your merchant account, they'll provide you with three strings of text, consisting of a SiteID, Key and Name. When you first go to run a transaction in the Virtual Terminal, you'll see places to fill-in those three strings:




Simply type the strings into the provided spaces (or, better yet, copy and paste from the email they send), then click on the *Save* button.

Your terminal is now capable of running transactions (at least those that are manually keyed in). In fact, even for swiped transactions (fully optional), little more is required. [1]

# *Chapter 4*

## Acquiring a Card Reader

Swipers (aka MCR devices; stands "magnetic card reader), EMV chip readers, and the like are generally the best way to run transactions (although, to be sure, it's very easy in the Virtual Terminal to key-in card information).

In today's world and for mobile contexts, the best device is Cayan's Genius Mini. It's tiny (fits easily in a pocket or on a neck lanyard), is wireless, and features no fewer than three read modes (it can swipe, EMV-chip read and read proximity cards). You should check with Cayan for details on fee levels.[2]

---

[1] In regard to merchant credentials, there is a potential complicating factor if you're running more than one business via the same Windows login, if you're using the Virtual Terminal for each such business, and if you want to have the transactions for each business run on different merchant accounts. There is a solution, at least in the integrated-within-ServiceDesk context. For details, please open this document: http://rossware.net/MiniManuals/VirtualTerminal_MakingCredentialsUniqueToBusiness.html.

[2] As of May 2018, only the Windows version of Virtual Terminal has been coded to work with the Genius Mini. We hope to have the iOS version similarly coded soon. In fact, sometimes after we accomplish goals we forget to come into here and update, so it may well be long since done at the time you read this. We similarly plan to code for use with the full-size Genius, but (at least at time of this writing in May 2018) that is not yet done.

A benefit in using an EMV chip-reader is your customers cannot get away with fraudulently claiming they did not authorize use of their card for swiping. This is not likely to happen. However, we have heard of instances where an EMV card was swiped as opposed to being chip-read, and the customer deliberately took advantage by knowingly claiming falsely that they never provided their card to you. In that situation, it doesn't matter how much proof you are ready to provide otherwise: the credit card company will adjudicate against you (ironically, this is not the case if you have keyed-in the transaction). [3] Anyway, if you use the EMV-chip-reading method instead of swiping, you are safe from this.

If you are satisfied with the prospect of a mere swiper, for Windows applications, we recommend buying the *Magtek 21040140*. It is tough, super reliable, and offers the convenience of being able to swipe in either direction and with the card facing in either direction. You do not have to get these from Cayan. Instead, we recommend you Google "21040140", and find the best deal currently available (likely about $50 per unit). There are a few cheaper Magtek models available, but you won't save much, and we think the benefits of the 21040140 are well worth the tiny difference. We recommend against picking any brand aside from Magtek for use with Windows products. Certainly some others might work, but with Magtek-standard devices you can be confident.

If wishing to use a mere swiper in the iOS environment, it must be the *ID Tech Shuttle*. Again, we recommend that you simply Google for the best deal on this unit (likely around $42). Unless you are acquiring directly from Cayan (which certainly makes sense if the price is right), be sure to pick a unit that does NOT have encryption (if in fact you decide to acquire from Cayan, encrypted is fine).

# *Chapter 5*

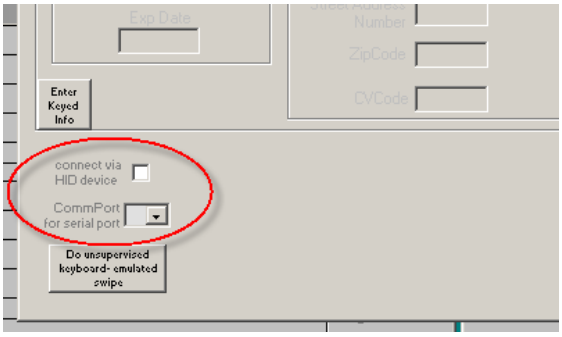
## Installing and Using an MCR ("Swipe") Device

In general, you need to do just two things, and the sequence does not matter:

Connect the device to your computer, using whatever method is applicable (i.e., if it's a USB device, plug into a USB port, if it's a serial device, plug into a serial port).

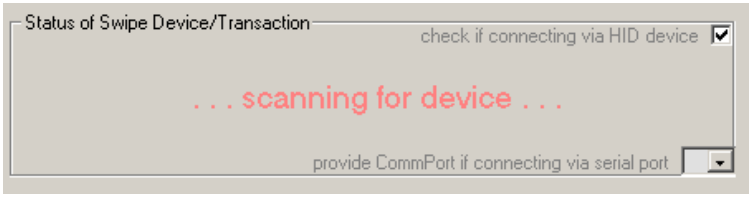
In the bottom-left corner of the Virtual Terminal, provide appropriate indication for the kind of device/connection that's involved:

[3] Of course, you could seek to have the consumer criminally prosecuted for criminal fraud (of which they are certainly guilty in such a case), and/or you could sue in small claims court. Regardless, neither is what you want to have to do.

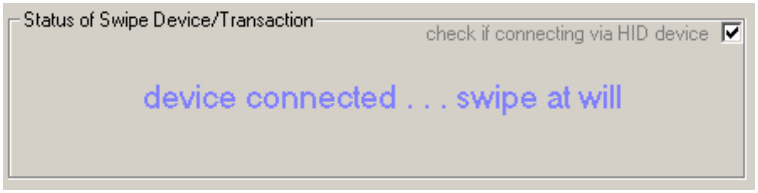



Specifically, if you're using a USB-connecting device, check the box so indicating. If you're using a device that connects via serial port,[4] provide the applicable CommPort number in the box provided.

That's it. Once the Virtual Terminal knows the kind of device, it will search:

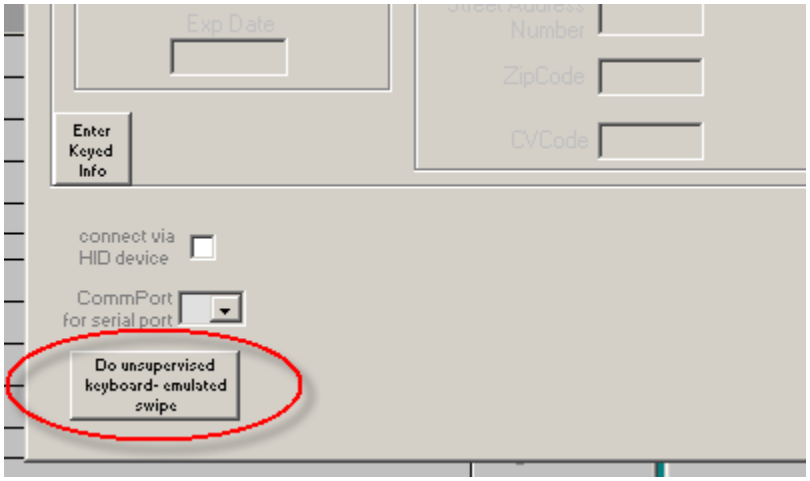



and upon locating the device, will alter its display to let you know.




There is one potential exception. It will arise if you happen to have picked a swiper the Virtual Terminal fails to detect upon scanning (this will happen only with non-Magtek brands). If you encounter this situation, there is a fallback position—at least if your swiper is designed to emulate keyboard input (in other words, as you swipe, data from the card automatically goes into any text-capable environment that your Windows cursor is in). For that situation, we have one more button:

[4] In regard to serial connections, and if you happen to use BlueTooth to connect with your swiper, please note the experience we had using our Printek via Bluetooth. We found that, though BlueTooth is the method of communicating between the external device (in this case the Printek printer/swiper) and computer, communication from that point onward (i.e., within the computer itself) is via a *virtual serial-port*. This "serial port" required a little setup within the Bluetooth configuration window. So far as we know, other swipers that communicate via Bluetooth may use the same method. At least, it's something to check if you choose BlueTooth.




Quite simply, for the described situation, you can click on that button, then swipe your card. (Please note the button will not be visible if you've indicated the system should look for either a USB or CommPort-type device).

# *Chapter 6*

**Running Actual Transactions**

This is quite self-explanatory. There's an obvious section in the interface for typing in credit card info. You'll use that section if not swiping, and otherwise leave it blank. If you are swiping, instructions on that are, essentially, embedded in the interface. Really, it's tough to go wrong, but if anything confuses you, feel free to give us a call (800-353-4101).

If you're using Virtual Terminal as a stand-alone application, you'll likely need no more instruction.

On the other hand, if you're using Virtual Terminal via its embedded integration in another Rossware product (e.g., ServiceDesk, SD-Mobile or SD-RevenueBuilder), there are some significant details regarding embedded use. You should read about these. They are contained in this document:

http://rossware.net/MiniManuals/VirtualTerminalIntegratedUse.pdf

# *Chapter 7*

**Staying Up-To-Date**

Rossware updates its products very frequently. There are always things that can be improved, and it's a constant effort at Rossware to do this, in every place we can.

If you are using Virtual Terminal within a larger Rossware application, there is no need to worry about separately updating Virtual Terminal. So long as you've kept the larger application up-to-date, you'll automatically have the latest version of Virtual Terminal embedded within—and there's no need to read further in this section.

If, however, you're using Virtual Terminal as a stand-alone product, we strongly suggest you check periodically to see if a new and improved version is available.

In fact, even if you just installed Virtual Terminal (i.e., from a mini-CD), it's a very good idea to check. CDs have a long shelf-life, after all, and it's possible you got one that was made some time back.

Regardless of the circumstance, to do updates, you'll first need a username and password from Rossware. Just call or email for the purpose (800-353-4101 or karie@rossware.net), and they'll set you up.

To check for an update, go to the Rossware website (www.rossware.net). Down in the bottom-left corner of the main page, click on *Updates*. When the next page displays, click on *Virtual Terminal*. This opens the Virtual Downloads page, and will show you the date and version of current update offered. If it's newer than what you're currently using, do the update (instructions are provided on the same page, but it's very simple).

# *Chapter 8*

**Reviewing Your Transactions On-Line**

As part of your setup, Cayan will provide you with log-in credentials for an on-line interface where you can attend to many elements of managing your account, including reviewing transactions, running reports, and things of that nature.

It's a powerful tool, and easy to use. There's not much more we need to say about it. It's important, simply, for us to make you aware it's there—and that you should use it.

# *Chapter 9*

**Assuring You Have an Awesome Deal**

We picked Cayan because, on the basis of careful study, we became convinced it was the best processor to recommend. However, you should not (at least in the long-term) take our word for this. You should verify it for yourself.

A very important part of any merchant processor relationship is how much you're paying. This can be very confusing. The problem is that a processor might quote you a very low "discount rate," but make up for it with other fees that are

thoroughly exorbitant, with result that your overall rate ends up being a very lousy one.

There's a simple way to end the confusion, at least when you're examining after the fact. What you want to do is calculate a simple figure we call the "*Net Effective Rate*." To get this figure, take any statement from any merchant processor, look to see what was the total amount processed during the month, and what were the total charges assessed by the processor. Take the total charges and divide by total amount processed. This will give you the Net Effective Rate.

For example, suppose that in a given month XYZ Corp ran $25,000 in total credit card charges. All of the charges on the company's statement totaled at $825. If you take the $825 and divide it by $25,000, you get .033 – which means XYZ Corp paid a Net Effective Rate of 3.3 percent (simply move the decimal two places to change the decimal fraction into a percent figure).

We explain this because we very much want you, after you've received your first couple of months' statements from Cayan, to calculate your net effective rate. Then do the same for the last preceding couple of months from your prior processor. We're betting you'll be very pleased with the comparison, and we're anxious to hear your report.

# *Chapter 10*

## PCI Compliance

In response to a series of well-publicized security breaches that occurred in the late 90s (consumer credit card data was nefariously stolen as sales were conducted at some major department stores), the Visa and MasterCard organizations created a consortium to create and enforce new and improved security standards.

The consortium is known as the "*Payment Card Industry Security Standards Council"*. As one of many consequences stemming from its efforts, every merchant that processes credit cards must now engage in a process that demonstrates its compliance with a set of minimal security standards.

This is called "*PCI Compliance*." Its difficulty and expense can range from significant (prox $600 or more) to quite minimal, depending on circumstances. Fortunately for those working with Cayan, the latter has arranged for certifications at a cost of just $59. Typically, certification is something that must be dealt with "down-the-line and eventually" rather than immediately upon setting up your merchant account.

Regardless of when you are compelled to certify, you should be aware of the general concerns that compliance review and testing are designed to address. At

core (and so that you know), the PCI Council wants to assure merchants are maintaining practices that minimize the possibility of cardholder data falling into nefarious hands.

Please be assured, there is nothing in Rossware's Virtual Terminal that ever saves any such data. It is deliberately configured as only a pass-through device. It uses cardholder data only momentarily, as it's provided, and after the transaction retains no trace of such data elements anywhere. So far its own usage is concerned, all such data simply evaporates (poof, it's gone), as the transaction is concluded (it was only there in the most transitory state, to start of with). For such reason, you may rest assured you are secure, so far as it is concerned.

A. Other Internal Data Storage.

The fact that Rossware's Virtual Terminal never saves cardholder data is good. But that by itself is not good enough. Just because the Virtual Terminal is not saving such data elements, it does not mean you could not do so independently — nor that, if you did, you would not run afoul of PCI Compliance objections by so doing.

For such reason, we highly suggest that you make a strict internal policy against ever storing cardholder data (specifically, credit card number, security code, and/or specific name as attached) in any context anywhere. In other words, assure you only use these data elements on-the-fly, during an actual transaction as input direct to the Virtual Terminal, and that you do not save them in any manner.

In addition, you should further assure there is nothing *otherwise* in your software systems, hardware and/or practices that might even potentially (and perhaps without direct intent) retain such data elements.

As an example, you might (potentially) have a key-logging program installed on a computer that's operating the Virtual Terminal. If so, that program in itself would capture a credit number as it's keyed in by a user, making it potentially vulnerable to abuse. To guard against that, you should assure that any computer that's operating Virtual Terminal does not have anything resembling a key-logging program simultaneously running on it.

As another example, when an operator keys-in a credit card number (i.e., rather than swiping), the keyed-in number shows momentarily within the box where he or she has typed. Potentially, your employee could use a screen-capture action to save an image of that number. The Virtual Terminal provides significant protection by masking any corresponding CVCode (if provided by the user) — so it can never show simultaneous with the card number itself (swiped data, of course, is never displayed, period). But even so, you should adopt policies that prohibit screen capture in these circumstances — to assure that even an image of the card number remains in a "never-saved" state within your system.

If your operational imperatives are such that you *must* store cardholder data, there is nothing in the PCI standards that outright prohibit doing so. However, you should carefully consider two strong factors that argue against it: (1) Rossware's Virtual Terminal will not assist you (again, it has no credit-card-data-saving functions at all); and (2) any separate practice you make, of saving such data, will make PCI certification into a much more complex and onerous process. If stored, such data must be subject to many protections (encrypting, careful isolation within secure servers, access logging, etc.) — all designed to assure that persons with nefarious intent never gain access. You're likely to find that to structure your systems in a compliant manner, and to adequately demonstrate such compliance, are no easy tasks. For *most* operations, at least, it will be much easier to simply refrain from ever putting such data anywhere that it's retained.

Again, Rossware's Virtual Terminal follows this policy scrupulously. It has since its first inception, and for such reason there is no need or concern about removal of any past/historical data as connected to it. It has never saved anything, in the past or now, that was then or is now a security concern. It has, in short, always been a "clean" system.

B. Audit Trails and Logging.

When your PCI audit is performed, you'll likely be asked about access logs. Virtual Terminal does not involve itself with any. The reason is that access logs have — as their fundamental purpose — the function of keeping track of who has accessed stored/sensitive data, when they did it, what their action was, and so on. Since Virtual Terminal does not involve itself with any such stored data, the subject of access logs is simply not applicable to its direct use (though, of course, if you otherwise /independently store such data, it will then be a concern – but not of the Virtual Terminal, since it is not involved in such storage).

C. Security Against Outside/Malicious Intrusions.

Another element of inquiry during your PCI audit will concern whether your system is vulnerable to penetration by malicious outsiders. In fact, the auditing entity will likely make attempts to get into your internal system from the outside, essentially pretending (for the purpose of testing) to be some hacker with malicious intent (if the auditor succeeds, you'll definitely flunk the test).

On the one hand, your security against such penetrations is arguably inapplicable to PCI concerns, since (at least presumably) you have no stored credit card data, to be potentially accessed (certainly, none as stored by the Virtual Terminal).

However, it's an excellent practice to assure your system is secure against such intrusions, regardless.

In this regard, you should (and as an example) assure your various login passwords (Windows Administrator, Router, etc.) are changed from the factory defaults (hackers use the defaults all the time, and shockingly often with total

success). Make sure you don't have any accounts beyond those strictly needed (more accounts make more potential paths for intrusion). If you maintain a wireless router, be sure it's set to use strong encryption, secure logins, etc. Make sure you always have a firewall. Further details, of course, are available in the PCI DSS Requirements Manual.

Outside the concern for keeping stored data secure (again, there should be no such data) against unauthorized outside access, there is also a concern about transmission of data within your network, across a wireless LAN, during the course of a transaction (another reason any wireless router needs to be securely configured). Regardless, so long as you are using such data solely within the Virtual Terminal (i.e., not typing it elsewhere within your system), you should be very secure. The data is securely encrypted for communication with Cayan (in such context the data might "fly in the air" between a particular wireless station and your wireless router, but it's encrypted regardless, so is invulnerable in that context). And (again, so long as you do not separately save it), there will be no other context for it to "fly-in-the-air" through your LAN (as there would in fact be, for example, if you typed and then saved the info in an application that saves data on your server). Once again, for multiple layers of security, this speaks to the fact you should only enter such data in the context of the Virtual Terminal.

D. Secure Updates.

The PCI Council is also concerned to assure that every credit processing system is secure against updates that might compromise security. If, for example, our Virtual Terminal was configured so that Rossware Computing could self-initiate an update — within your system, but via actions taken here — it would conceivably be possible for a person of nefarious intent to simulate those mechanisms, and thereby replace your good and secure copy of Virtual Terminal with a counterfeit purposely designed to extract credit card data for fraudulent purposes.

Our strategy against this vulnerability is simple. As described in Chapter 7, updates are initiated solely by you, acting directly on your own deliberate accord, via downloads from our secure website. Indeed, since there is no provision of any "remote-access technology" (i.e., via which any outsider could accomplish the update for you), PCI concerns in this area are, in fact, not directly applicable.