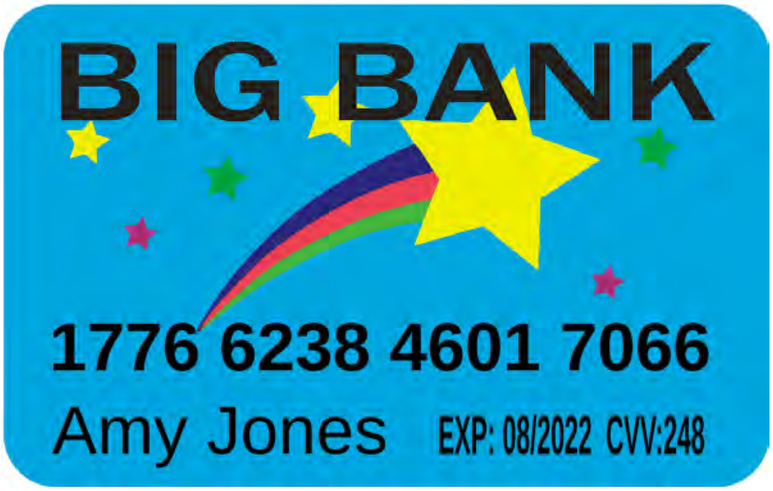
NC3 THE NO COMPROMISE CHARGE CARD

The Charge Card



This little piece of plastic is central to most of us. Whether debit or credit, charge cards are displacing cash and checks in our daily lives.

You can use them in person at the store or the gas station.

You can use them over the telephone or over the internet. You can write them on a bill. You can get cash with them.

Participants

Consumer	that's you!
Merchant	someone selling you goods or services
Provider	provided the charge card you are using

Charge Card Parts

The critical card parts are your name, the account number, expiration date and that three or four digit number called the *Card Verification Value*, or CVV for short. Usually the CVV is on the back with the magnetic stripe that holds other data and everything else is on the front. Sometimes just your name is on the front and everything else is on the back. Doesn't really matter where they are as long as they are all there.

All that information is generally in plain-text.
You (and anyone else who is looking) can read all of it.

Who Can Use Your *Charge Card*?

The charge card is a powerful and easy to use tool and that is a big problem; it may be too powerful for its built-in safety. Say someone steals your charge card then pretends to be you. At the store someone might notice that this big fella here does not really looks like an "Amy Jones" and an attentive clerk might ask for another piece of identification. (Wouldn't it be nice if crooks all wore stripes? The high tech crooks look more like students, lawyers, accountants, or just like us.) But then, someone might *not* notice.

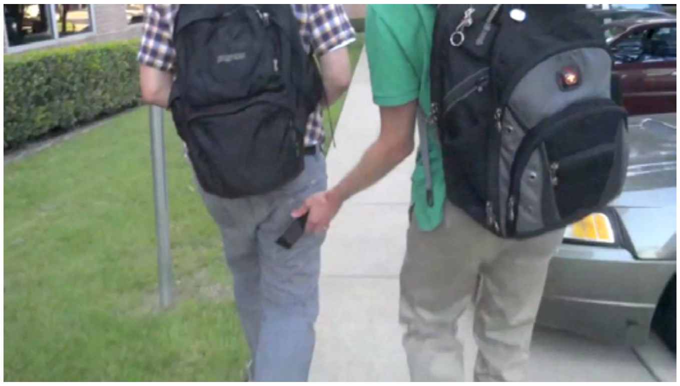
Who Can Use Your Charge Card *Information*?

Your physical card doesn't have to be stolen for someone to get enough information to charge something to your account.

Small

Anyone who has your card in their possession for more than a few seconds could write down the information. That includes your waiter, the clerk at a drive-through, anyone.

Medium



If your card has an RFID tag, devices are available so that someone can scan your card information from a distance. The card stays in your wallet or purse, but the information is compromised.

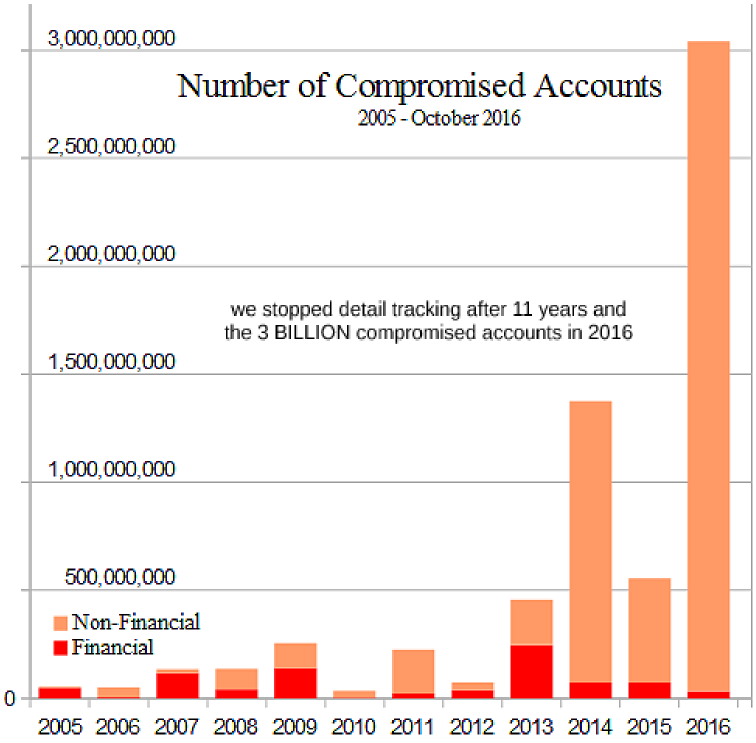
Large

More industrious crooks have other devices. You know those plastic folders that contain your restaurant charge slip? They can contain card scanners. The card swiper at the store? More than a few have been hacked.

Extra Large

The really high volume of charge compromises come from hacked merchants or service bureaus who retained your charge card information.

From 2005 through 2016 there were **829^{+} million** compromised financial accounts and another **5.5^{+} billion** compromised non-financial accounts which can provide confidential information for identity theft. Over 3 billion accounts were compromised in 2016 alone!

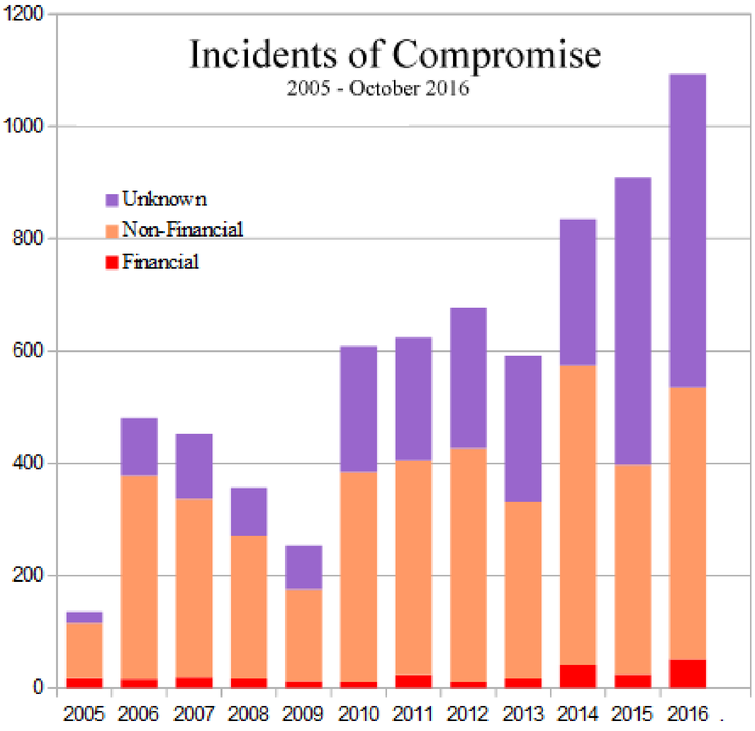


we stopped detail tracking after 11 years and the 3 BILLION compromised accounts in 2016

There were over 7,000 recorded incidents of compromise including over 2,680 incidents of compromise where the number of affected persons was not revealed.

Rules about who is required to report what to whom and when differ between jurisdictions.

Companies are reluctant to make disclosures unless they are required.



All we really know is that compromises *continue* to take place.

Current Interfaces

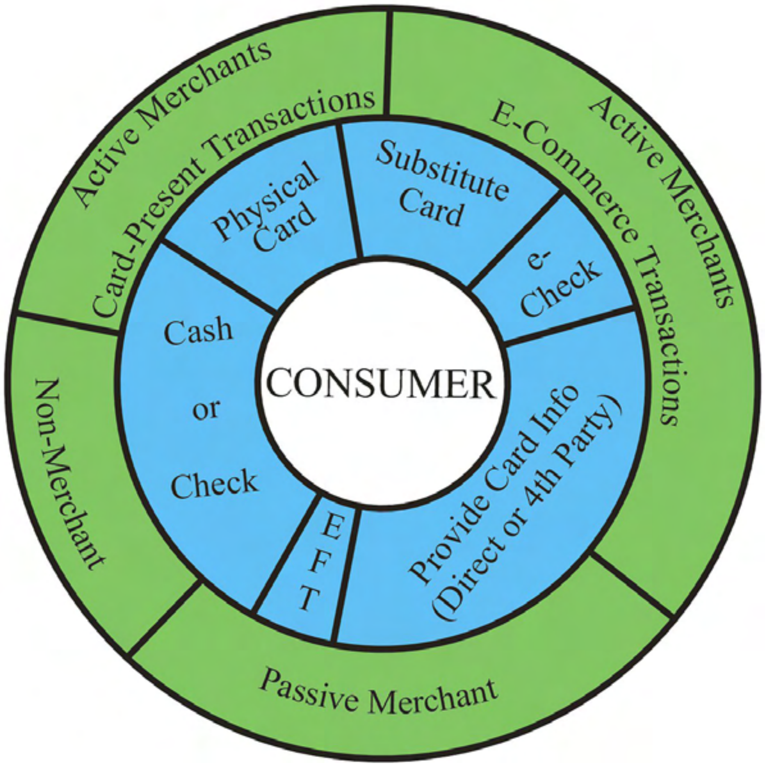
Consumers can pay merchants many ways.

Active Merchants – Card Present

This is where you are in the physical presence of the merchant, like at a grocery store. You pay these merchants with cash, check or a physical card or substitute.

Active Merchants – E-Commerce

You can't use cash so you provide card information, a substitute card for one-time use, e-check, or use a fourth party who has your card information and provides something else to use.



Passive Merchant

These are merchants who are neither physically nor electronically in the same place as the consumer when the transaction takes place. A utility bill, received on paper, would be from a passive merchant. You can pay passive merchants with cash, check, electronic funds transfer (EFT), provide your card information directly or via a fourth party.

Non-Merchants

These include other people and organizations that don't take charge cards. You generally use cash or check.

Why NC3?

NC3 was designed to…

- ✔ increase the security of commerce by reducing consumer exposure
- ✔ increase functionality to provide for new capabilities
- ✔ make transactions easier for consumers, merchants and providers alike
- ✔ reduce transaction time and increase frequency of touch-less operations
- ✔ reduce capital, operating and risk-related costs for merchants & providers

These are done in a framework with one fundamental principle:

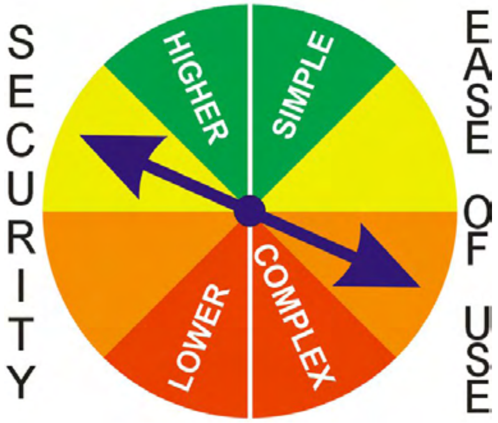
information is provided to those who need it

and no one else!

What NC3 Is & Isn't

NC3 is a *new way of thinking* about security for consumers, merchants and providers that works *within* the existing communications and transaction infrastructure while adding new functionality to make life easier for all the participants. It breaks the inverse relationship between *security* and *ease of use*.

Existing Systems

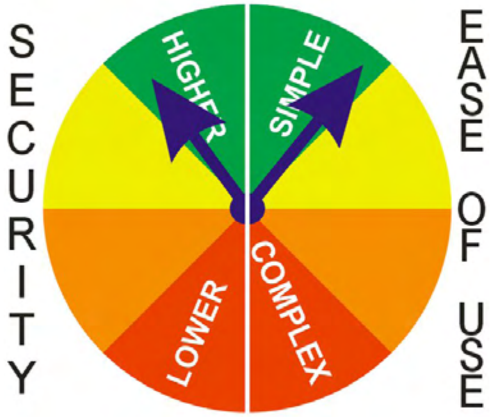


As security of a system increases the use of that system generally becomes more complex.

Also generally true: The easier a system is to use, the less secure that system is.

This *inverse* relationship forces a choice: High security **or** easier to use.

NC3



By increasing security automatically without requiring additional consumer involvement NC3 breaks the inverse relationship allowing higher security **and** simplicity for a more secure system that is also easier to use.

Thus, this is the

No Compromise Charge Card.

NC3 is not a new kind of key or vault. It isn't an add-on, or a separate service, or a fourth-party provider. It isn't an additional piece of technology or super-card. It is a new way of thinking, using something you probably already have.

NC3 Concept

There are many security systems for charge cards. There are companies who sell monitoring services. There are special one-time charge cards for electronic (computer based) or mobile (cell-phone) use. There are battery powered super-cards providing one-time use numbers. There are fourth parties who accept your real charge card information and provide you something else to use at merchants.

These deter, but don't always stop, the crooks!

NC3 started as a question:

If crooks are going to crack the vault,
why put jewels there in the first place?

If the critical account information *isn't* in the transaction information, but merchants can still get paid, then even if the card information is compromised the underlying charge card number can't be compromised ***because it isn't there!***

In human terms: **what people don't know, they can't reveal.**

Many financial protection solutions are based on better locks and better vaults; these may delay, but not defeat, the most skilled crooks.

Removing the jewels means even if the crooks get into the vault they are denied their prize. *NC3 does not retain, therefore can't communicate, the consumer's underlying charge card number to the merchant,* thereby increasing consumer security and decreasing merchant data breach liability. Phrased as a statement:

What Merchants don't have,
Crooks can't steal!

Security

Separation Of Identification and Authorization

BIG BANK
All plain text
Identification and
Authorization
Amy Jones
V:951

A charge card provides a visible charge account number **and** a provides information for a context-free authorization. Literally the account number, expiration date, name and other information on the card can be used without constraint.

NC3 uses an NC3 identifier which, on its own, *cannot* authorize a transaction.

A separate transaction-adaptive (context sensitive), dynamically content-rich, authorization is created especially for that particular transaction and useful for no other.

Identifier and authorization are separately encrypted. Even if the encryption were cracked, your real account number and other confidential information exists *only* at your provider. So even if the NC3 identifier is revealed the bad guys don't have your account information.

Reducing Fraud Costs

Provider expenses and losses are passed back to the merchants as part of fees. Merchant losses are reflected in their pricing. In the end the consumer pays. Preventing the crime (as opposed to potential recovery afterward) saves thousands of hours and considerable law enforcement resources.

Identifier

Existing Charge Card - Account identifier and associated name are printed in plain text on the card. The full number has only recently been omitted from receipts. The account identifier is *always* available and visible on the card.

NC3 - The NC3 identifier is a unique consumer identifier, different from the account identifier. This consumer identifier is *insufficient* to authorize a charge.

Authorization

Existing Charge Card - The name, card number, expiration date, and credit verification value can be used to authorize a transaction.

NC3 – Any one authorization can be restricted to a single merchant, for a specific amount (or a not-to-exceed amount) for a specific date and time limit.

Can a Copy be Used?

Existing Charge Card - **Yes**. Using the implied authorization described above, multiple purchases can be made.

NC3 - **No**. That explicit authorization is restricted to that specific merchant, amount, etc. Duplicates of that authorization are rejected. This means that altered swiper devices (skimmers etc) pose less of a threat.

Trust

Existing Charge Card – The consumer *implicitly* trusts that what they expect to be charged will be charged. This is “trust” because the merchant can charge something else and does, sometimes by accident, sometimes on purpose.

NC3 – Consumers *explicitly* and *automatically* set the approval amount within the encrypted authorization. Attempts to charge something else will not be approved.

Awareness

Existing Charge Card – You may never know that someone or something has illegally copied your charge card information until the extra charges show up on your bill – possibly *weeks* or *months* after the information was stolen.

NC3 – You are going to notice the absence of your phone *a lot* faster.

Code Only Compromise Not Possible

Any code, such as personal identification code (PIN), can be compromised. The NC3 system has code elements, but they require the consumer's device to be useful. *Information alone* cannot create a NC3 authorization.

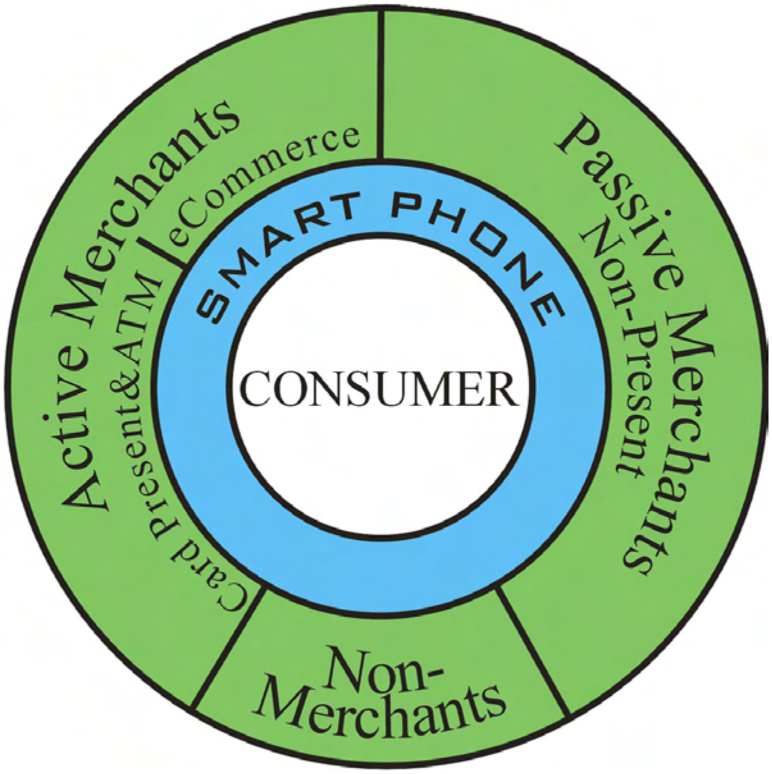
Reverse Engineering Not Possible

An NC3 identifier is *not* created using the underlying charge card number. So, even a compromised NC3 identifier *cannot* be reverse engineered. The underlying charge card number ***just isn't there!***

Established Consumer Protections

This isn't charging items to your smart phone, this is another way to use your existing charge card accounts. This is important because consumer protections for fraudulent use of debit and credit cards are well established. Charging to (not via) your cell phone is a new venue. Telephone providers are neither providers nor banks and their consumer protections are less beneficial to consumers.

Benefits



Easy Single Interface

NC3 is a single solution providing increased security for **all** transactions.

Every smart phone with a camera can use NC3 **right now**.

Special chips are *not* required.

You *don't* need internet access to make a transaction.

Operational efficiencies arise for consumers, merchants and providers.

Merchants need a smart device with a camera and *zero additional equipment.*

ATMs? Sure! Think about displaying a transaction on your smart phone and presenting the phone's screen for scanning. The touch-less transaction is executed and you're done. Card skimmers have no card to skim.

Does not reduce existing capabilities

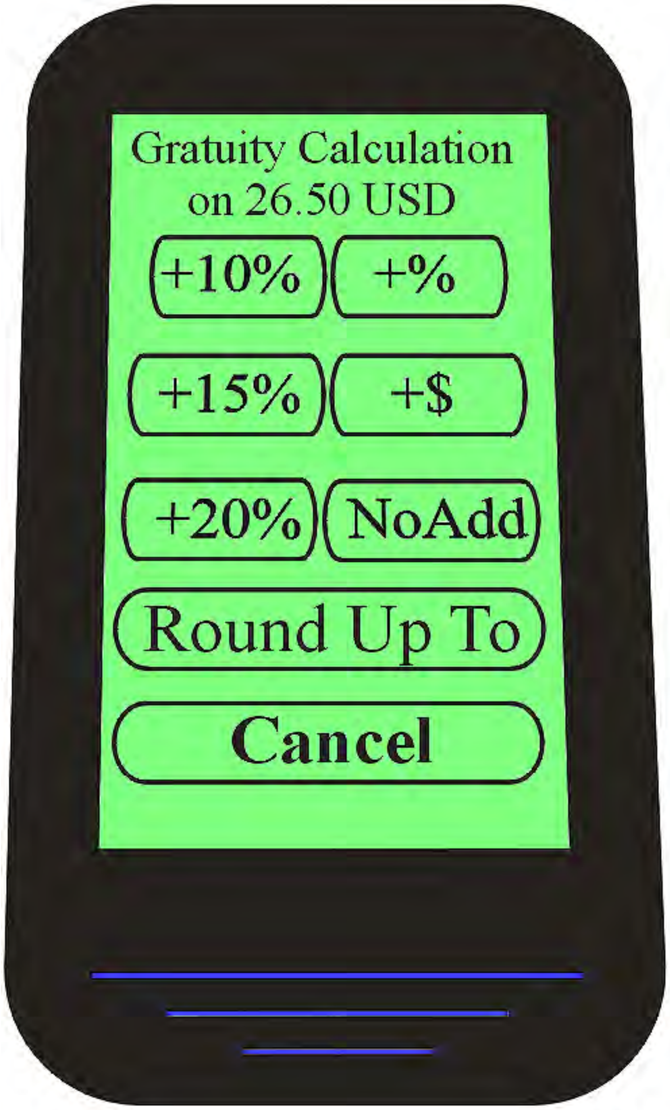
Some “solutions” generate one-time card numbers. Great if you are making a one-time charge. What about using your charge card for a repeating authorization? Say once a month? Or once a year? Or, some merchants take your multiple item order then bill as each item ships. You can't authorize those transactions if the card number can be used just once. NC3 allows for a restrictions on frequency of re-use, a not-to-exceed value, restriction to a single merchant, a self-expiring date and more to keep the security and the functionality.

New Capabilities

These are just a few of the many new consumer capabilities NC3 provides.

Other Payments

NC3 works for all forms of commerce including card-present, electronic, mobile, paying a paper utility bill, scanning an ad from video or print media, and more. NC3 requires nothing more than a stock smart phone, no special chips or internet access.



Gratuity Calculator

A merchant can request a gratuity with an invoice. When the consumer goes to pay, a little calculator pops up with easy options to add a predefined percentage, a different percent, a dollar amount, round up to a chosen amount and more options.

Person to Person Payments

Within the framework of security, efficiency and increased functionality, NC3 makes Person-To-Person-Payment transactions straightforward.

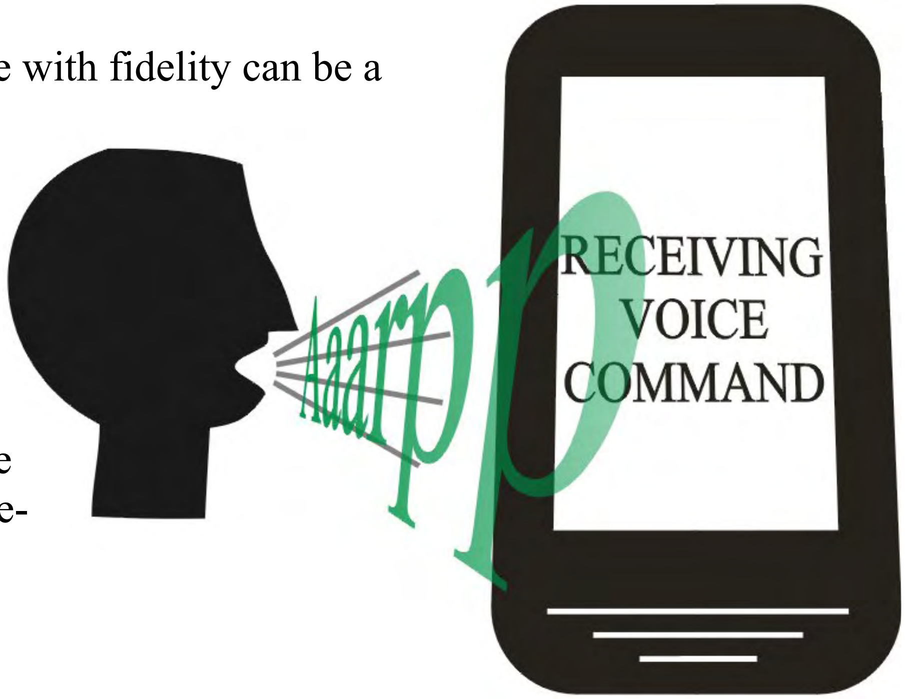
Sub Accounts

NC3 makes creation of sub-accounts easy. The card holder can allocate a fixed amount for other family members. No more students draining your credit for beer and pizza!

Voice Command

Any sound you can reproduce with fidelity can be a command.

See web site under *How It Works | Examples* for *NC3-Ex-VoiceCmd-OrderInAdv* example where I order a large coffee (double cream, no sugar, please) and an apple fritter using my AARP freebie-donut coupon.



Audio Assistance Mode

NC3 can be configured to request and receive approvals via voice making NC3 helpful for the visually impaired.

Currency Awareness

International transactions are handled with ease. Each NC3 account has “native account currency” (NAC) which is used for billing and reconciliation. Initially that is the same as the “default transaction currency” (DTC) for transactions. Each time a merchant requests charge in another currency the consumer is asked to accept the change. The consumer can change the DTC to avoid the questions.

Affiliation Code Locker

Loyalty programs often include a key ring or wallet sized tag. NC3 can capture that tag and link it to the merchant. The *Affiliation Code Locker* (ACL) as the one place to keep shopping cards, club cards and other affiliations. Affiliation codes can be shown stand-alone, at the same time as a charge approval, and included in the transaction approval itself. All done easily and securely.

Straightforward to Implement

For Physically Present Merchants

NC3 uses optical transmission readable by optical coupon scanners. Small or mobile merchants can use their own cell phone as scanners. Once the consumer's authorization is received at the merchant's point of sale (POS) it can be transmitted within the same communications environment already in use. Small or mobile merchants can communicate via WiFi or text messaging. Consumers just *scan, approve and pay*. There is no need to implement near field communication (NFC), EMV, radio frequency identification (RFID), or other expensive systems at physical presence merchants.

For Electronically Present Merchants

The merchant only needs to display the customized billing code. The consumer can scan that code either by using their smart phone scanner, or, if they are shopping using their smart phone, the code can be captured without scanning. Once approved, that payment is encrypted and transmitted via text message.

End the time-consuming, error-prone process of typing names, account numbers, addresses, special security codes etc. Consumers just *scan, approve and pay*.

For Passive Merchants

Passive merchants just have to print the bill code on your invoice and send it via physical mail or via email. You scan it, approve it and your payment is transmitted via encrypted text message. No transactional internet access required.

Reduce postage expense and delay in getting paid. Email the invoices, save money and reduce carbon emissions from postal delivery vehicles. Consumers don't have to start a secure browser, surf to their payment site, log in, set up merchants, or type in the amount. Just *scan, approve and pay*.

Table of Contents

For reference information see

http://nc3.mobi/references

Look under *How It Works* for many examples.

http://nc3.mobi/how-it-works

To get these advanced security and great features make your voice heard.

Tell your provider!

How? See *How To Get NC3* on www.NC3.mobi

http://nc3.mobi/how-to-get-nc3

Our goal

Make

Charge Card Information Theft

a profitless crime