Real World eCommerce for ColdFusion Developers

Lawrence Cramer

Application Dynamics Inc | Cartweaver.com

Lansdowne Resort, Leesburg VA August 12- 15, 2009

www.cfunited.com

Overview – elements of eCommerce

A. Technical
   - Code considerations
   - Database options
   - Security

B. Logistical
   - Transactions – how to get the money & what to do with it.
   - Security and Liability

eCommerce – It’s a different Ball Game!

A. Assuming the consultant's role!
   - What to be aware of
   - Protecting yourself
   - Protecting the client
   - Protecting clients from themselves!

Technical – looking at your options

A. **If I only had a brain!**
   - What is “statelessness”
   - The Stateless Web and what to do about it
   - The Cart requires a state – or memory

B. ColdFusion’s options to make the web remember

Technical – Sessions

- Pluses
  a) Memory resident, therefore they are Fast.
  b) Can contain complex data such as arrays and structures.
- Minuses
  a) Do not persist (time out after set time period)
  b) Do not persist from server to server (cluster)
  c) Does Not Support Shared SSLs – see “b”
  d) Increase server load and can slow things down

Technical – Client Variables or Cookie

A. Pluses
   - Require very little server memory
   - Can persist from visit to visit.

B. Minuses
   - Cookies can be turned off by the user
   - Limited Size
   - Contain simple data (string).

Technical – Hybrid Solutions

A. Bring a Database Into the Mix

As long as you depend on some kind of relationship between the server and the browser there is a potential for failure. If you want to be absolutely sure there are additional steps you can take.

- Write the Cart to the database with a UUID and set a Session or Cookie or Client Variable with the same UUID to keep the user and Cart in sync.

Technical – Hybrid Solutions cont.

- Pluses
  a) Persists as long as you want it to
  b) If the Session or Cookie are deleted you can have the user "sign in" to re-link with the Cart.
  c) Gives you a record of what people are placing in their carts. Even if they don't buy
- Minuses
  a) Increases Database Load
  b) Increases Database Maintenance
  c) Additional Code complexity
  d) Can be slower (although marginally)

Technical – States Overview

A. Pick the solution that's Best for you.
B. Look Ahead!
   - It is important to not over engineer your application
   - It’s important to not under engineer it.
   - Go ahead and start out simple but be sure what you set up is extendable.
   - Be sure you don't paint yourself into a corner.

Technical – Databasics

A. **THE decision** you are going to have to live with for a long, long time.

B. “Damn it! I'm a web developer, not a Database engineer!“

- **That may be true, but if you are developing E-Commerce applications you are going to HAVE TO know how a database works and how to work with them.**
- **This topic alone is enough to fill several sessions so we are only going to cover the basics.**

Technical – File Databases! (MS Access)

A. Pluses
   - Cheap
   - Easy to run and learn
   - Portable

B. Minuses
   - Not secure
   - Very limited capacity & speed
   - Limited number of concurrent users
   - Only moderate data integrity

Technical – Database Servers

A. Common Database Servers are MS SQL SERVER, MySQL, Oracle, Postgres…
   - Pluses
     a) Fast
     b) Very robust
     c) High Data Capacity
     d) Large Number of Concurrent Users
     e) Greater Data Integrity
     f) Very Secure

Technical –Database Servers

A. Minuses
   - More Complex
   - More Learning Curve
   - Setting up local development / testing environment more involved
   - Host Must Support Your Choice

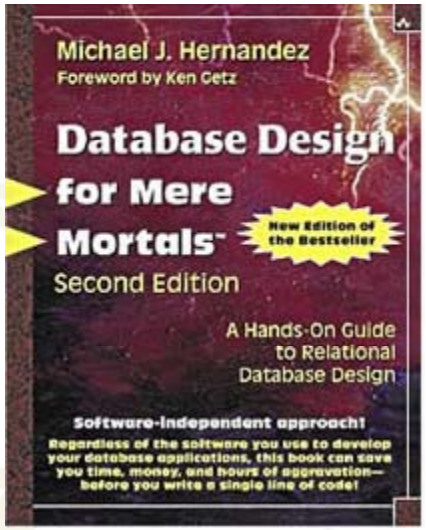
Technical –Database Servers

A. **The Logical Decision**

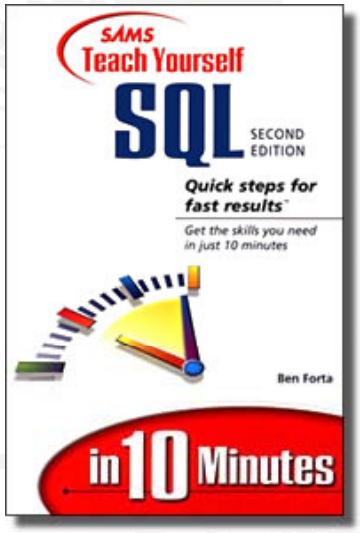
- Time to put on your consultant's hat!
- Database Servers are the only *serious* option.
- MS Access is the most commonly used database on the web.
- Don’t contribute to this problem! Strongly advise your clients against it.

Technical –Databasics

A. Two Invaluable Resources!



Database Design for Mere Mortals: A Hands-On Guide to Relational Database Design, Second Edition – by Michael J. Hernandez



Sams Teach Yourself SQL in 10 Minutes (2nd Edition) - by Ben Forta

Technical – Security

A. Protect Your Customer's Data, and Protect Yourself

- There are serious issues to consider. Even capturing someone's credit card data temporarily is a risk. Storing it in your Database is even a bigger one.
- **The merchant and the developer bears the responsibility of showing "Due Diligence"** in protecting a customer's credit data. Let's look at some security measures that MUST be taken.

A. Here are a few points we will consider

- Protect Data In Transit - SSL
- Protect Customer Credit Card Data
- Secure Your Database

Security - SSL

- An SSL (Secure Socket Layer) Encrypts your pages and accompanying data when it is requested by your browser. It will only be unencrypted and viewable by the same browser that requested it. If anyone along the way should intercept the data packets it will be un usable.

A. Two Primary SSL Options
   - Shared SSL
   - Private, Purchased SSL

Security – SSL- Shared

Some ISPs will make a "Shared SSL" available to their customers. The ISP shares its SSL with you by placing your Secure pages on its SSL protected server.

A. Pluses
   - Cheap
   - For the most part as secure as an individual SSL
   - Easy to set up. The ISP already has it set up, they just internally map part of your site through their SSL Server.

Security – SSL- Shared

A. Minuses

- You Aren't Listed As The Certificate Owner. This can shake consumer confidence and loose sales.
- Cannot be transferred if you move to a different host
- Since Shared SSL requires a transfer to or through a separate server, many session based carts will not work.
- Appear less professional

Security – SSL- Individual/Purchased

When you purchases your own SSL Certificate, the issuing company generates a unique SSL "code" or "key". This code has to be sent EXACTLY as it is to your ISP to be set up on your site. It is set up and mapped to your site's IP Address.

A. Pluses
   - Bolsters consumer confidence. The SSL is registered to your company
   - If you change ISPs you take SSL with you.
   - The SSL is installed on your site, no server transfer or switching required. This avoids session problems.

Security – SSL- Individual/Purchased

A. Minuses
   - Cost More. Not nearly as much as it used to though. An SSL can be had for under $100 a year.
   - More is involved in setting it up, though knowledgeable ISPs can make the process quite painless.

Security – SSL

A. **Conclusion… Get Your Own!**
   - This is an another area where the client may pushback to save a few bucks.

B. **Convince them to do it right!**
   - Point out that the name on the SSL cert not matching their business name will cause shoppers to leave. How many sales can they afford to lose?

Logistical

A. **That's the "Technical" side…**
B. **What's the "Logistical" side**

Other stuff you're going to have to know!

Logistical – Things You'll Need To Know

A. **Payment Gateways**
   - Real Time
   - Delayed Response
   - Intrusive - Plumber's Nightmares – Google Checkout & PayPal Web Payments Pro

B. **Merchant Accounts**
   - Separate from gateway
   - Integrated with gateway
   - Not always the same as the regular business bank account

Logistical – Processing Credit Cards

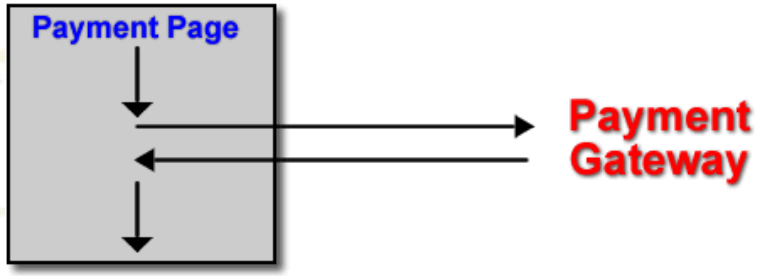
A. Has little to do with code

B. Is a beehive of activity – salesmen, new “products,” shifting rates

C. The client is going to be looking to YOU to be the expert and have the answers!

Logistical – Payment Gateways

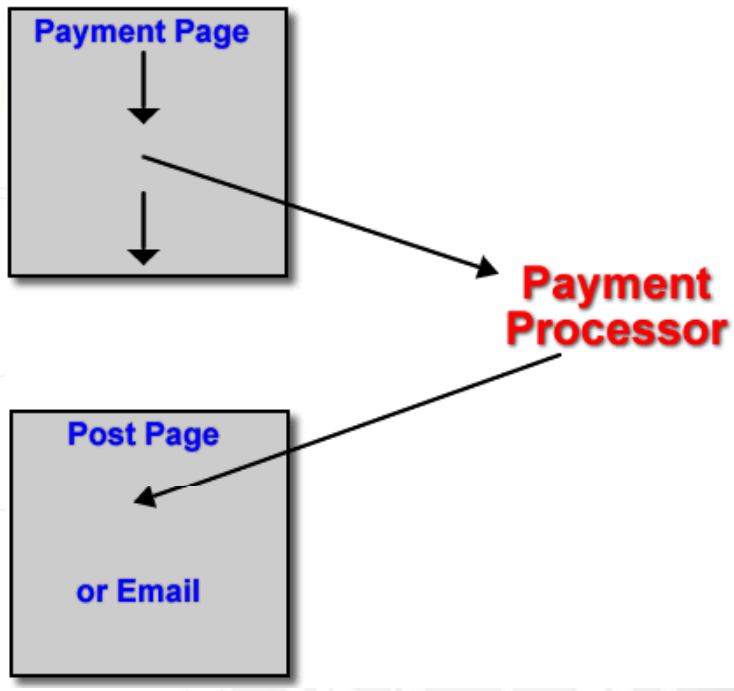
A. Real time



B. HTTP Post – XML – immediate response
C. Transaction continues based on response
D. Authorize Net, PayPal PayFlow Pro, LinkPoint & many more.

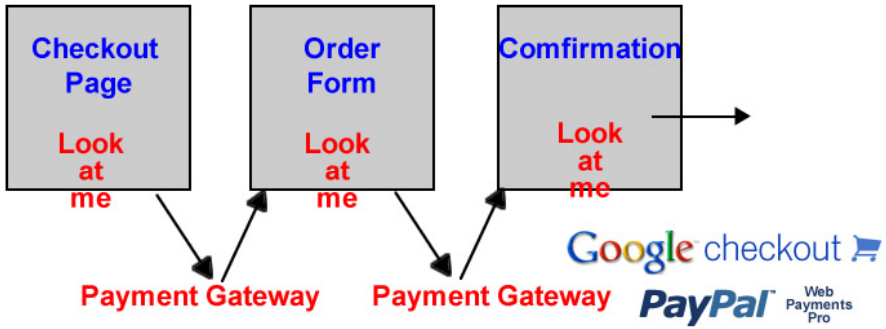
Logistical – Payment Gateways

A. Delayed Response
   PayPal Standard, WorldPay Junior
B. Transaction sent
C. Response is posted back later
D. Checkout continues "blind"
E. Can be worked with by posting back and updating the database.



Logistical – Payment Gateways

A. Oddball Proprietary Solutions



B. Multiple points of interaction throughout the checkout process

C. Intrusive Branding

D. Access to your customers for up selling / sign-up “opportunities”

Logistical – Payment Gateways

A. First Choice – Real Time
B. Second – Delayed Response
C. Last and positively least – Proprietary

D. Time to be a consultant again.
Make a strong case for the best choice – Real Time.

Logistical – Payment Gateways

A. How real time gateways work

```
<!--- USER SETTING  [ START ] ================================================== --->
<cfset variables.AuthNetLogin = ""><!--- Fill in your login --->
<cfset variables.TransactionKey = ""><!--- Fill in your transaction key OR password --->
<cfset variables.AuthNetPassword = "">
<cfset variables.TestMode = "True">

<!--- HTTP Post parameters ====================================================== --->
<cfhttp url="https://secure.authorize.net/gateway/transact.dll" method="post">
<cfhttpparam type="FormField" name="x_Login" value="#variables.AuthNetLogin#">
   <cfif variables.AuthNetPassword NEQ "">
   <cfhttpparam type="FormField" name="x_Password" value="#variables.AuthNetPassword#">
<cfhttpparam type="FormField" name="x_type" value="AUTH_CAPTURE">
Usually many more than this…
</cfhttp>

<!--- HTTP Post Back  parameters ================================================ --->
<cfset request.TransactionResult = Val(ListFirst(cfhttp.fileContent))>
<cfset Request.TransactionID = ListGetAt(cfhttp.fileContent, '7')>
<cfset request.TransactionMessage = ListGetAt(cfhttp.fileContent, '4')>

<!--- Set local variables based on HTTP Post parameters ================================ --->
<!--- 1=Pending, 2=Verified, 3=Shipped --->
<cfif request.TransactionResult EQ 1>
   <cfset request.TransactionResult = "Approved">
   <cfset request.OrderStatusID = 2>
</cfif>
```

Logistical – Payment Gateways

A. Fortunately they mostly work the same
   With the exception of Proprietary gateways – Google and PayPal Web Payments
B. Request Integration API and examples
C. Many have Authorize Net Emulation
   Authorize Net is a good standard to learn, and many services work exactly like they do.

Logistical – Merchant Accounts

A. Internet Friendly

This is not just a business Bank account, or credit card account. The kind of merchant account we are talking about is **one that is used to interfacing with a Payment Gateway**. Be sure to check if they support your Gateway provider.

B. Rates vary! Do your home work!

Rates can be very different from bank to bank. Often times it is less expensive to have a different Merchant Bank for your web site than for your business.

C. Package Deals are often easier to set up and offer better Rates.

Check with your Gateway provider to see if they offer a gateway/merchant account package.

Logistical – Merchant Accounts

A. Online Merchant Account and Business Bank don't have to be the same. (In fact usually aren't)

B. Be a Hero!

OK your a Web Developer and this is up to your client right?
By discussing these simple facts with your client you can be very popular when your advice in this area saves your client significant time and money.

C. A happy client is a paying client!

Security & Liability

A. **“Is it secret? Is it safe?”**

B. Evil Is Looking For Your Data!

Identity theft and malicious mischief are very wide spread on the web. We've talked about securing your data in transit, now make sure your database is safe.

C. The most secure data is data you don't have!

- On a shared host there is no way to totally secure your data!
- NEVER Store Credit Card data – Never

Be willing to go toe to toe with your client on this one

Security & Liability

A. PCI Compliance (Payment Card Industry)

The major credit card issuers created PCI compliance standards to protect personal information and ensure security when transactions are processed using a payment card. All members of the payment card industry (financial institutions, credit card companies and merchants) must comply with these standards if they want to accept credit cards.

B. 6 Categories of Compliance

- Maintain a secure network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

Security & Liability

A. PCI Compliant on a shared host, how?

1. Maintain Secure Network

   Talk to your host about their security measures, both on the server and the database. Specifically mention your concern about PCI. Also, purchase a good SSL and have it installed into the ROOT of your site.

2. Protect Card Holder Data

   SSL encrypt your credit card data and Get Rid Of It! – Pass it off to the payment gateway provider and do not store it in the database or in any variable form that lingers in a cookie or memory.

3. As for categories 3 through 6

   Choose a quality host and stay in contact with them. Frequently remind them that your site is an ecommerce site that that on-going security management of the server you are on and the database you are using is of paramount importance.

   Be a polite squeaky wheel.

Be Firm – Do What's Best For The Client

A. No Cheap Hosts
B. No Shared SSL
C. Never Store Credit Card Data
D. Dive in and learn about Merchant Accounts, Payment Gateways
E. Be willing to walk away if the client won't listen – Let some other developer get sued!

Conclusion

A. The technology/ coding (sessions, databases, emailing, HTTP Post) of an ecommerce site is really pretty basic.
B. The Presentation of an ecommerce site is getting easier with jQuery, and many of the new CF Ajax capabilities
C. Be willing to learn the non-developer's part of the business, embrace the role as a consultant
D. At all times – Think Real-World Security First!

Thank You!

Lawrence Cramer

CEO – Application Dynamics Inc | Cartweaver.com

lawrence@cartweaver.com

cartweaver.com

Blog.cartweaver.com

twitter.com/LawrenceCramer