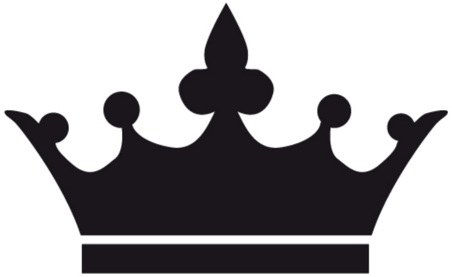


Cash is King
Who’s Wearing Your Crown?

Accounting Systems Fraud in the Digital Age

Tom Eston and Brett Kimmell

Agenda

- Introduction to Accounting Fraud
- Microsoft Dynamics Great Plains
  - Vulnerabilities and Attack Vectors
- Attacking the Users of Dynamics GP
- Fraud with Custom Malware (Mayhem)
- The Attacks: How to Commit Fraud
- Accounting Controls to Prevent Fraud
- Conclusions

About Your Presenters

Tom Eston

- Manager of the SecureState Profiling & Penetration Team
- OWASP Contributor
    - Mobile Threat Modeling Project Lead
    - OWASP Testing Guide v4
- SANS Mentor
- Security Blogger/Researcher: Spylogic.net
- Podcast Co-host: Social Media Security Podcast
- Speaker: Black Hat USA, DEFCON, ShmooCon, DerbyCon, SANS, MSI, OWASP AppSec

Brett Kimmell

- Manager of the Risk Management Practice at SecureState
- CISSP, CISA, CISM, CPA, CITP, PCI QSA
- Previously the Director of Information Systems and CFO for United Way of Summit County

Introduction to Accounting Fraud

When We Break In

- Penetration Testers and Attackers do this every day!
- Low hanging fruit
  (Apache Tomcat, JBoss, MS08-067)
- Easy to evade technical security controls
- Find the most sensitive data
  - Passwords, SSNs, PCI data, PHI, Proprietary
- Screenshot, Report, Profit, Repeat
- Nothing new here…

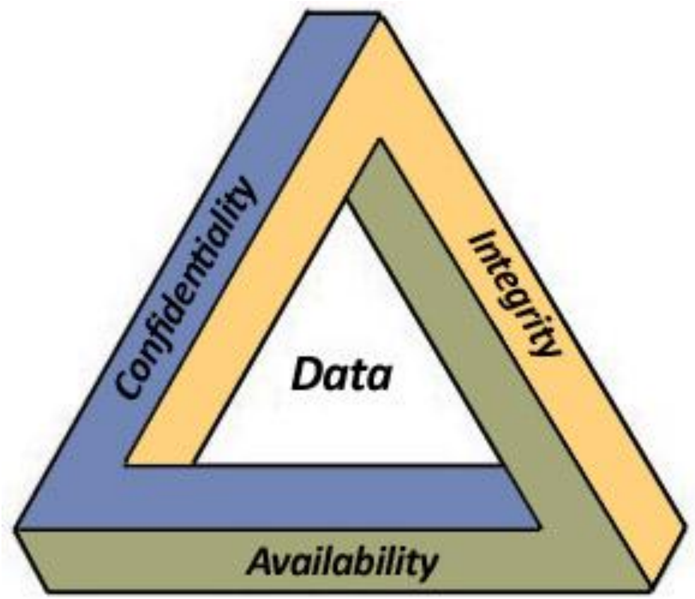
Photo Credit: http://cosine-security.blogspot.com/2011/10/derbycon-retrospective.html

What If?

- We could demonstrate ***real*** business risk?
- Typically this is financial risk and hits the bottom line of an organization
- Attack the accounting and financial systems
- We could test the non-technical accounting controls (not like an "audit")

Technical Controls 101

- **Confidentiality**
- **Integrity**
- **Availability**



Technical controls can only go so far.
When they fail (and they will) what do you rely on?

Accounting Controls 101

- Accuracy
- Timeliness
- Relevancy
- Reliability
- Consistency
- Comparability

The Problem?

- Accounting controls may not be in place
  - Or properly implemented
- Limited resources
- Limited skill set
- Limited time

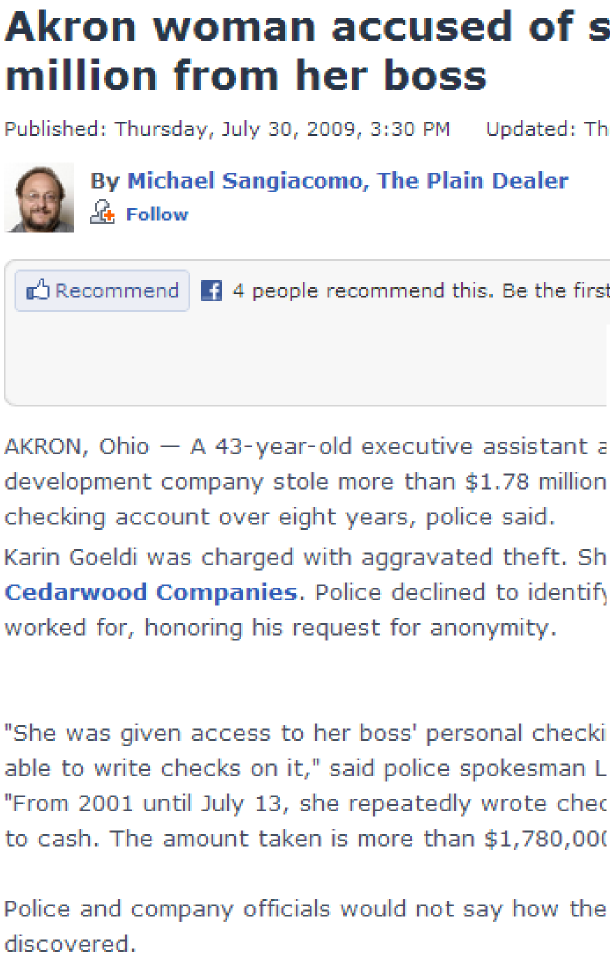
It’s very unlikely that accounting departments are reconciling every account each month!

Traditional Accounting Fraud

- Insider Embezzlement
- Overstating Profits
- External Check Fraud
- Insider Fraud
  - Kickback schemes, skimming, sales fraud, etc.

Primary Control: Reconciling Bank Accounts!

Accounting Fraud Examples



Akron woman accused of stealing more than $1.78 million from her boss

Published: Thursday, July 30, 2009, 3:30 PM   Updated: Thursday, July 30, 2009, 4:11 PM

By Michael Sangiacomo, The Plain Dealer

Follow

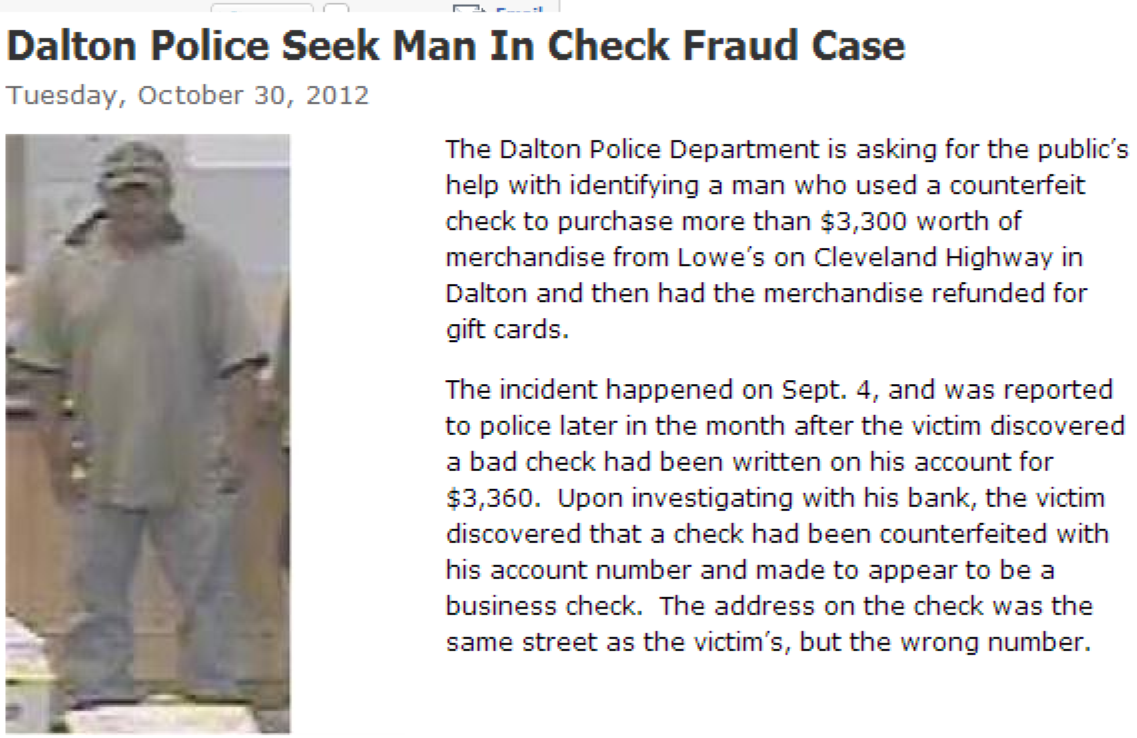
Recommend 4 people recommend this. Be the first of your friends. Comment 12 Share

AKRON, Ohio — A 43-year-old executive assistant a development company stole more than $1.78 million checking account over eight years, police said.

Karin Goeldi was charged with aggravated theft. Sh **Cedarwood Companies**. Police declined to identify worked for, honoring his request for anonymity.

"She was given access to her boss' personal checki able to write checks on it," said police spokesman L "From 2001 until July 13, she repeatedly wrote chec to cash. The amount taken is more than $1,780,00

Police and company officials would not say how the discovered.



Dalton Police Seek Man In Check Fraud Case

Tuesday, October 30, 2012

The Dalton Police Department is asking for the public's help with identifying a man who used a counterfeit check to purchase more than $3,300 worth of merchandise from Lowe's on Cleveland Highway in Dalton and then had the merchandise refunded for gift cards.

The incident happened on Sept. 4, and was reported to police later in the month after the victim discovered a bad check had been written on his account for $3,360. Upon investigating with his bank, the victim discovered that a check had been counterfeited with his account number and made to appear to be a business check. The address on the check was the same street as the victim's, but the wrong number.

Microsoft Dynamics Great Plains

Microsoft Dynamics GP

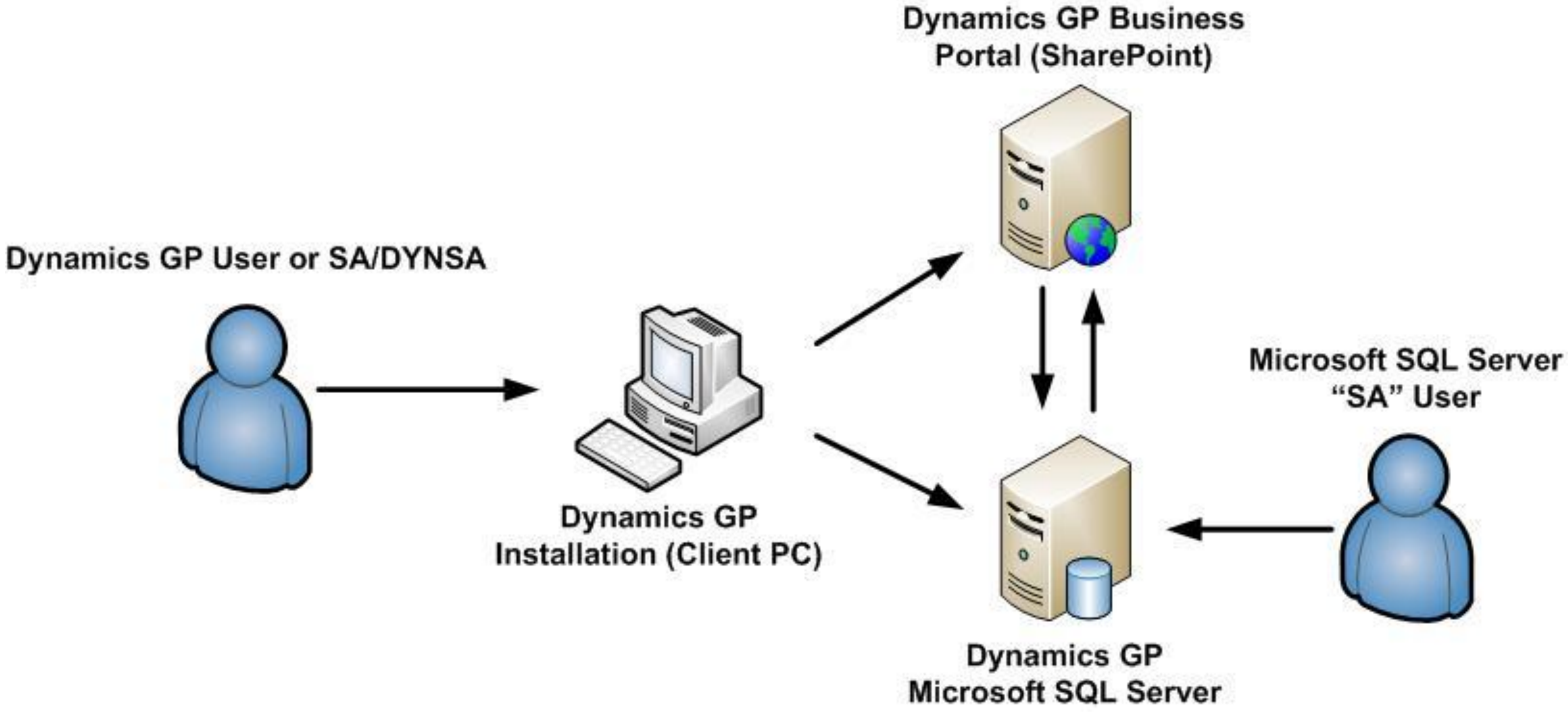
- One of the most popular accounting systems in the world for medium to large size businesses
- Microsoft purchased GP from Great Plains Software for $1.1 Billion in 2000
- Written in Dexterity specifically for GP
- As of 2010: 41,000 companies use GP

Microsoft
Dynamics GP

Microsoft Dynamics GP - Users

- No Windows Authentication (Active Directory) integration available (out of the box)
  - User accounts are created, managed and stored by SQL Server
- SQL Server “SA” account is the most powerful
- DYNSA owns all the GP databases. Performs privileged actions without the SA account in GP.
- Regular user accounts perform daily actions

Microsoft Dynamics GP


Dynamics GP Business Portal (SharePoint)
Dynamics GP User or SA/DYNSA
Microsoft SQL Server "SA" User
Dynamics GP Installation (Client PC)
Dynamics GP Microsoft SQL Server

- Uses "client-server" architecture
- Application runs on the client, not the server

Locating the GP Systems and Database

System Naming Conventions

- Conduct DNS or NETBIOS queries
- Network shares with GP client installation
- Typical names we’ve found on networks:
  - GP
  - GP-PORTAL
  - DYNAMICS
  - DYNAMICS_DB
  - GREAT PLAINS
  - ACCOUNTING
  - FINANCE

Additional Recon

- Most Critical: GP SQL Server
- Others systems include:
  - The GP client applications (user workstations)
  - GP Business Portal (SharePoint)
- Company Intranet
  - Usually reveals GP and/or accounting system documentation
- Network Shares
  - Sometimes the GP application is shared on the SQL server!

Attack Vectors in GP

Vulnerabilities in GP

- DoS and remote overflow vulnerabilities in GP version 9 and lower
- Weak cipher for the system password (2010)
  - Debunked by Microsoft as a real issue
- Typical SQL Server vulnerabilities and misconfigurations
  - Example: Local Administrator group added to the "sysadmin" role on the SQL Server

Attacks We Like for Fraud

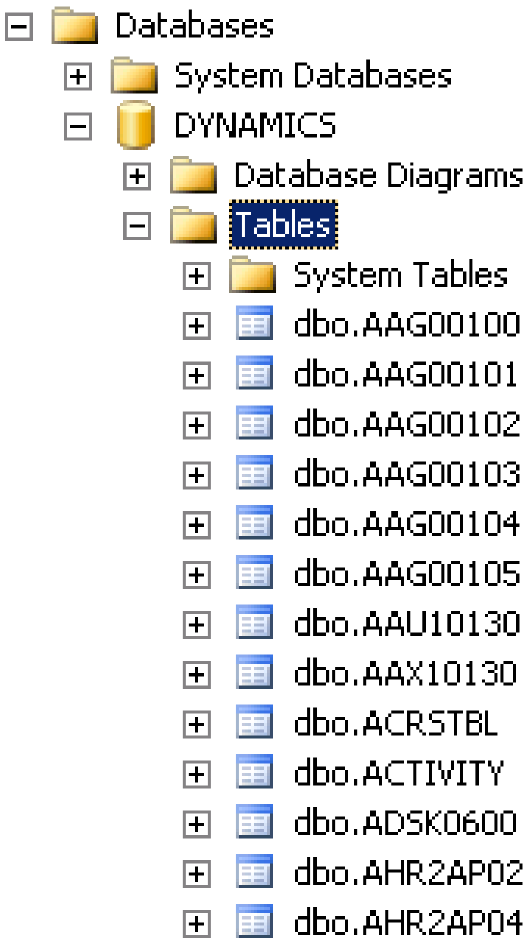
- Gain access to the GP SQL database directly
- GP user account hijack from the client
- Process injection via custom malware on the client

Attacking the Database

- Goal: Modify and create GP database entries to commit fraud
- Easy with direct access to the SQL server
- One problem…
- How do we know what to modify to commit the fraud?

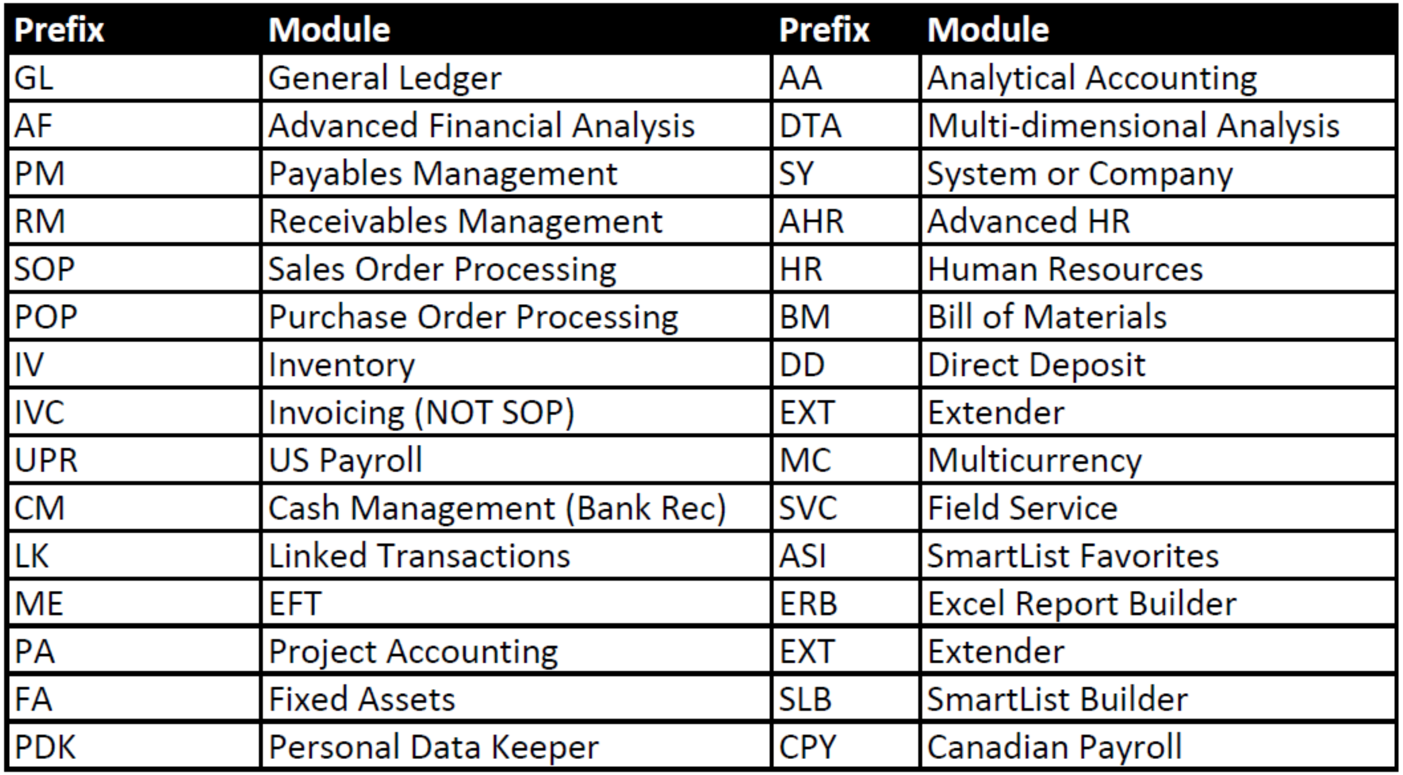
GP Table Naming Conventions

- GP Tables are not named with good descriptions…
- There is good news though!



- Databases
  - System Databases
  - DYNAMICS
    - Database Diagrams
    - Tables
      - System Tables
      - dbo.AAG00100
      - dbo.AAG00101
      - dbo.AAG00102
      - dbo.AAG00103
      - dbo.AAG00104
      - dbo.AAG00105
      - dbo.AAU10130
      - dbo.AAX10130
      - dbo.ACRSTBL
      - dbo.ACTIVITY
      - dbo.ADSK0600
      - dbo.AHR2AP02
      - dbo.AHR2AP04

GP Table Prefix Identification



Prefix	Module	Prefix	Module
GL	General Ledger	AA	Analytical Accounting
AF	Advanced Financial Analysis	DTA	Multi-dimensional Analysis
PM	Payables Management	SY	System or Company
RM	Receivables Management	AHR	Advanced HR
SOP	Sales Order Processing	HR	Human Resources
POP	Purchase Order Processing	BM	Bill of Materials
IV	Inventory	DD	Direct Deposit
IVC	Invoicing (NOT SOP)	EXT	Extender
UPR	US Payroll	MC	Multicurrency
CM	Cash Management (Bank Rec)	SVC	Field Service
LK	Linked Transactions	ASI	SmartList Favorites
ME	EFT	ERB	Excel Report Builder
PA	Project Accounting	EXT	Extender
FA	Fixed Assets	SLB	SmartList Builder
PDK	Personal Data Keeper	CPY	Canadian Payroll

Credit: Leslie Vail
http://dynamicsconfessions.blogspot.com/2012/05/data-flow-and-table-names.html

GP Table Identifiers

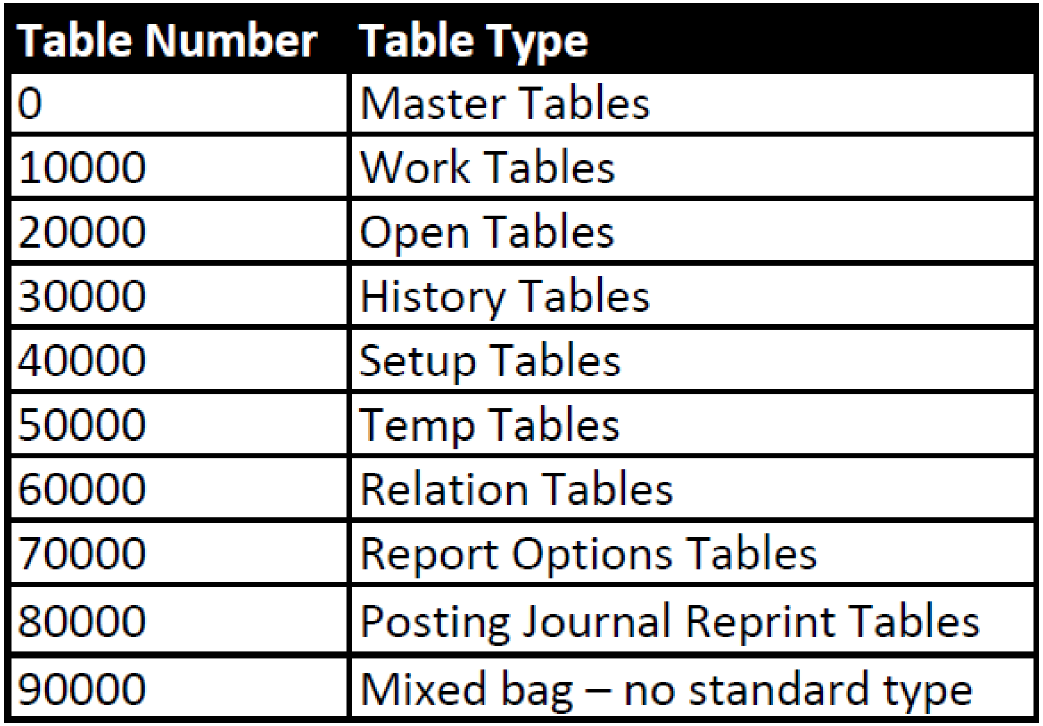


Table Number	Table Type
0	Master Tables
10000	Work Tables
20000	Open Tables
30000	History Tables
40000	Setup Tables
50000	Temp Tables
60000	Relation Tables
70000	Report Options Tables
80000	Posting Journal Reprint Tables
90000	Mixed bag – no standard type

- Put the prefix with the identifier to determine the table function
- PM1000 = Payables Management Work Table

Attacking the GP User

Who to Target?

- Accounting Department Users
- Controller
- Bookkeeper
- CFO
- The Accountant

The Goal

- Compromise the user’s workstation
  - GP application is installed there!
- GP login and password
- Compromise other workstations, pivot to the accounting users
- Create backdoor into the user’s workstation(s)

Example Scenario

- Harvest accounting department usernames and emails via LinkedIn
- Create targeted phishing email
- Link to download malicious attachment
  - “Click here to install the latest GP patch!”
- Mayhem ensues…or installs (more on this in a minute)

Creating the Perfect Fraud via Custom Malware

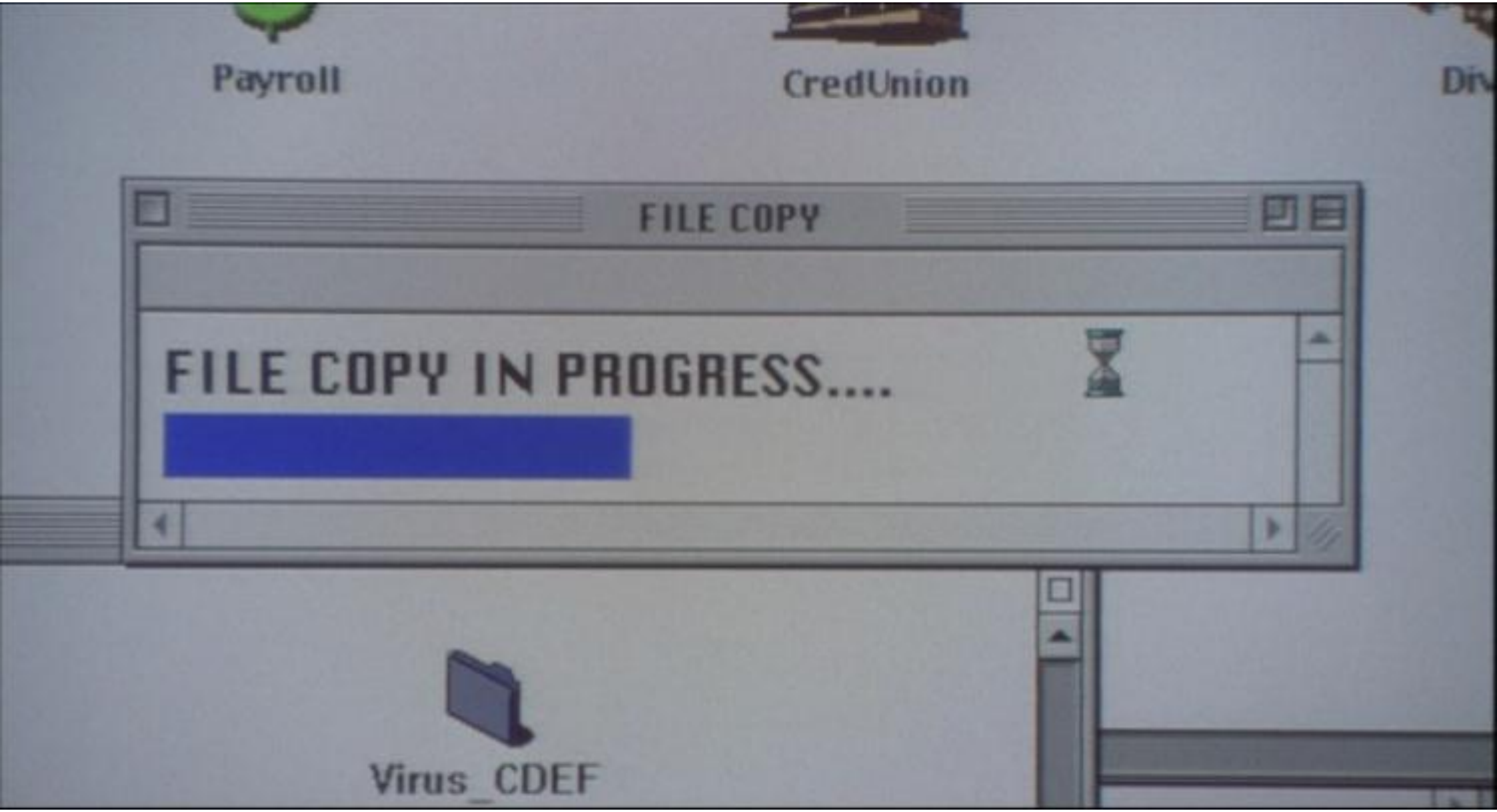
Who Wants to Create Mayhem!

- Who’s seen the “Office Space” Movie?
- Considered a “cult classic” from a Hollywood perspective
- Install virus (via floppy disk), infect accounting system, shave off a fraction of a penny of each transaction, check account balance, profit!

Office Space ©1999 Twentieth Century Fox

Office Space ©1999 Twentieth Century Fox

Office Space ©1999 Twentieth Century Fox

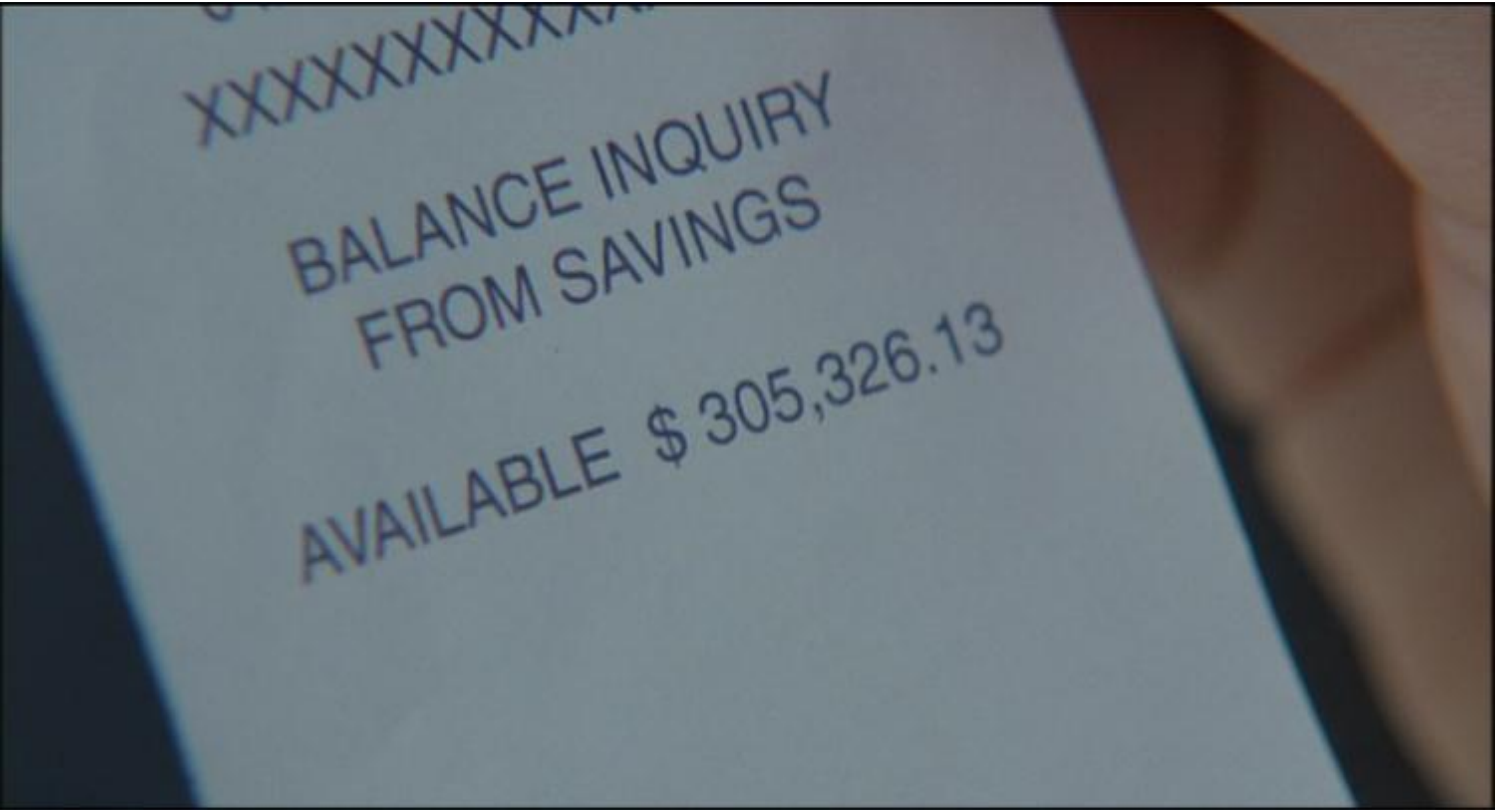


FILE COPY

FILE COPY IN PROGRESS....

Office Space ©1999 Twentieth Century Fox

$ PROFIT $



XXXXXXXXX

BALANCE INQUIRY
FROM SAVINGS

AVAILABLE $ 305,326.13

Office Space ©1999 Twentieth Century Fox

Introducing: Mayhem Malware

- Proof of Concept code created by Spencer McIntyre of the SecureState Research & Innovation Team

How Mayhem Works

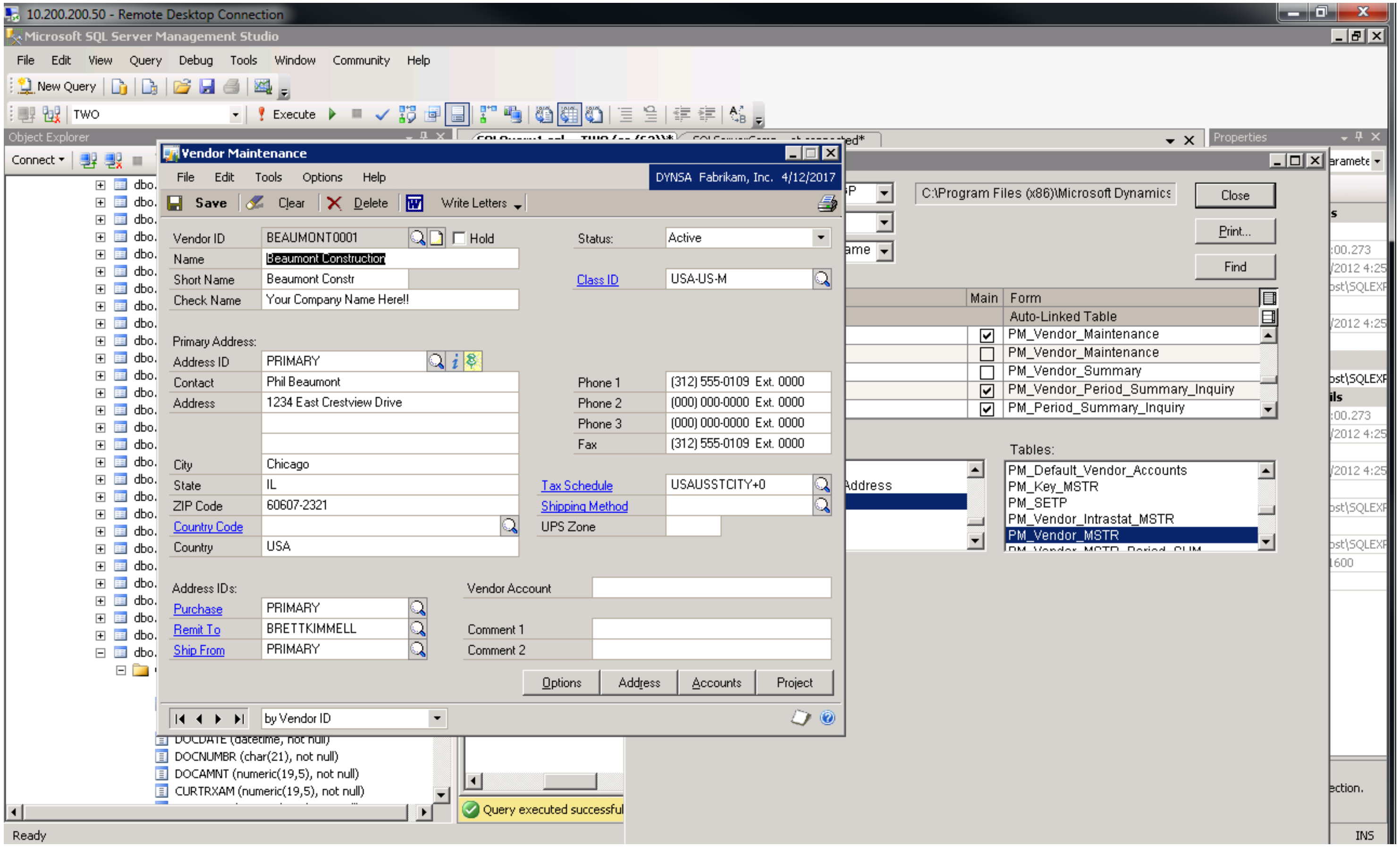
- Uses function hooking and library injection to execute within the context of the GP frontend
- Goal: Open a channel back to the attacker so commands can be made via the GP frontend
- Mayhem is injected at runtime and can use patching techniques

How Mayhem Works

- Mayhem creates hooks in key locations
  - Most important: calls to ODBC32 library
- Mayhem monitors this and then allows injection of SQL commands into the database as the *authenticated user*
- A HTTP backdoor is created which allows on the fly modification of SQL commands by the attacker
- More details on Mayhem in our whitepaper

The Attacks:
How Fraud Can be Committed

Manipulating Existing Vendor Records' Remit-To Address



10.200.200.50 - Remote Desktop Connection

Microsoft SQL Server Management Studio

Vendor Maintenance

DYNSA Fabrikam, Inc. 4/12/2017

Vendor ID	BEAUMONT0001
Hold	□
Name	Beaumont Construction
Short Name	Beaumont Constr
Check Name	Your Company Name Here!!
Status:	Active
Class ID	USA-US-M

Primary Address:

Address ID	PRIMARY
Contact	Phil Beaumont
Address	1234 East Crestview Drive
City	Chicago
State	IL
ZIP Code	60607-2321
Country Code	
Country	USA
Phone 1	(312) 555-0109 Ext. 0000
Phone 2	(000) 000-0000 Ext. 0000
Phone 3	(000) 000-0000 Ext. 0000
Fax	(312) 555-0109 Ext. 0000
Tax Schedule	USAUSSTCITY+0
Shipping Method	
UPS Zone	

Address IDs:

Purchase	PRIMARY
Remit To	BRETTKIMMELL
Ship From	PRIMARY
Vendor Account	
Comment 1	
Comment 2	

by Vendor ID

C:\Program Files (x86)\Microsoft Dynamics

Main	Form
	Auto-Linked Table
☑	PM_Vendor_Maintenance
□	PM_Vendor_Maintenance
□	PM_Vendor_Summary
☑	PM_Vendor_Period_Summary_Inquiry
☑	PM_Period_Summary_Inquiry

Tables:

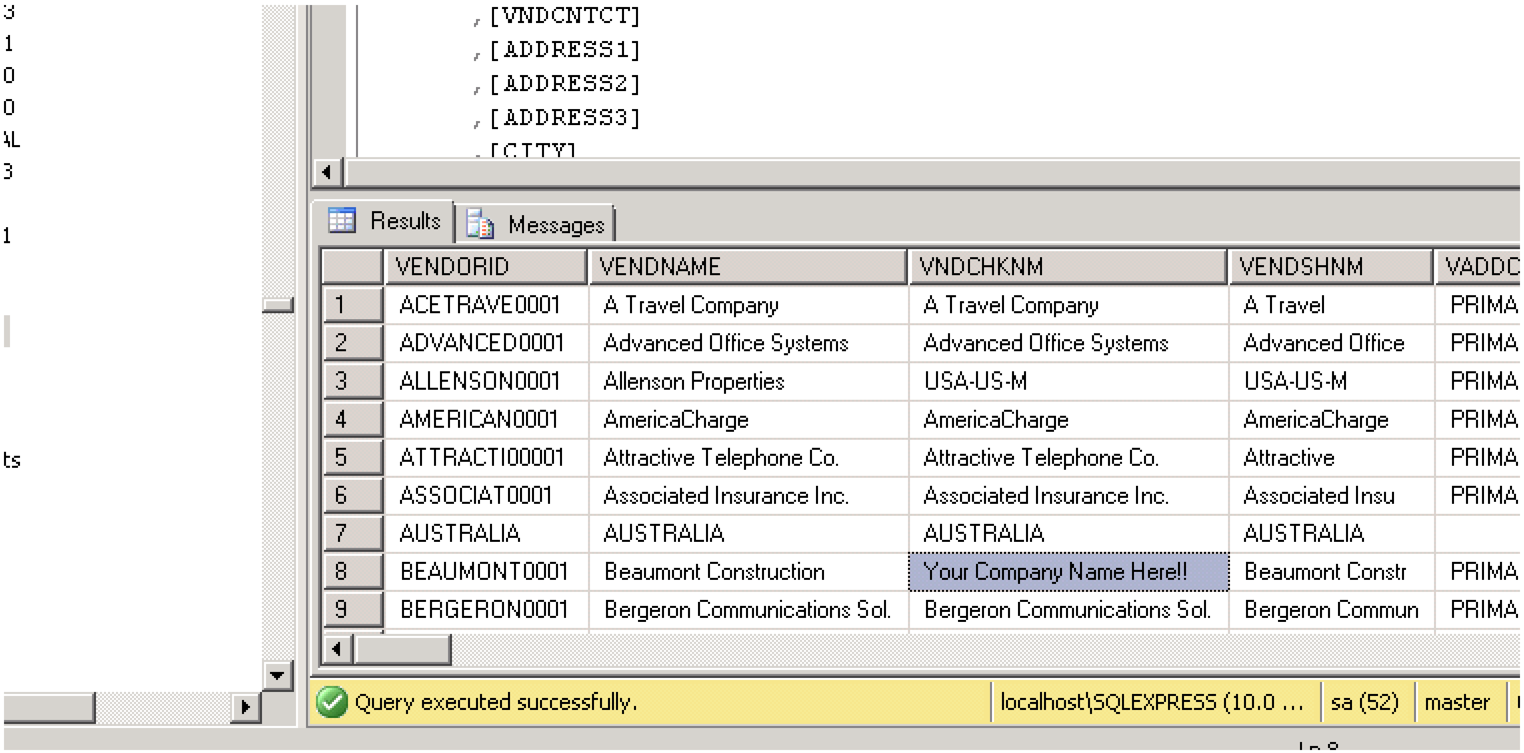
- PM_Default_Vendor_Accounts
- PM_Key_MSTR
- PM_SETP
- PM_Vendor_Intrastat_MSTR
- PM_Vendor_MSTR

DOCDATE (datetime, not null)
DOCNUMBR (char(21), not null)
DOCAMNT (numeric(19,5), not null)
CURTRXAM (numeric(19,5), not null)

Query executed successful

Ready

Manipulating Existing Vendor Records' Remit-To Address



3
1
0
0
AL
3

1

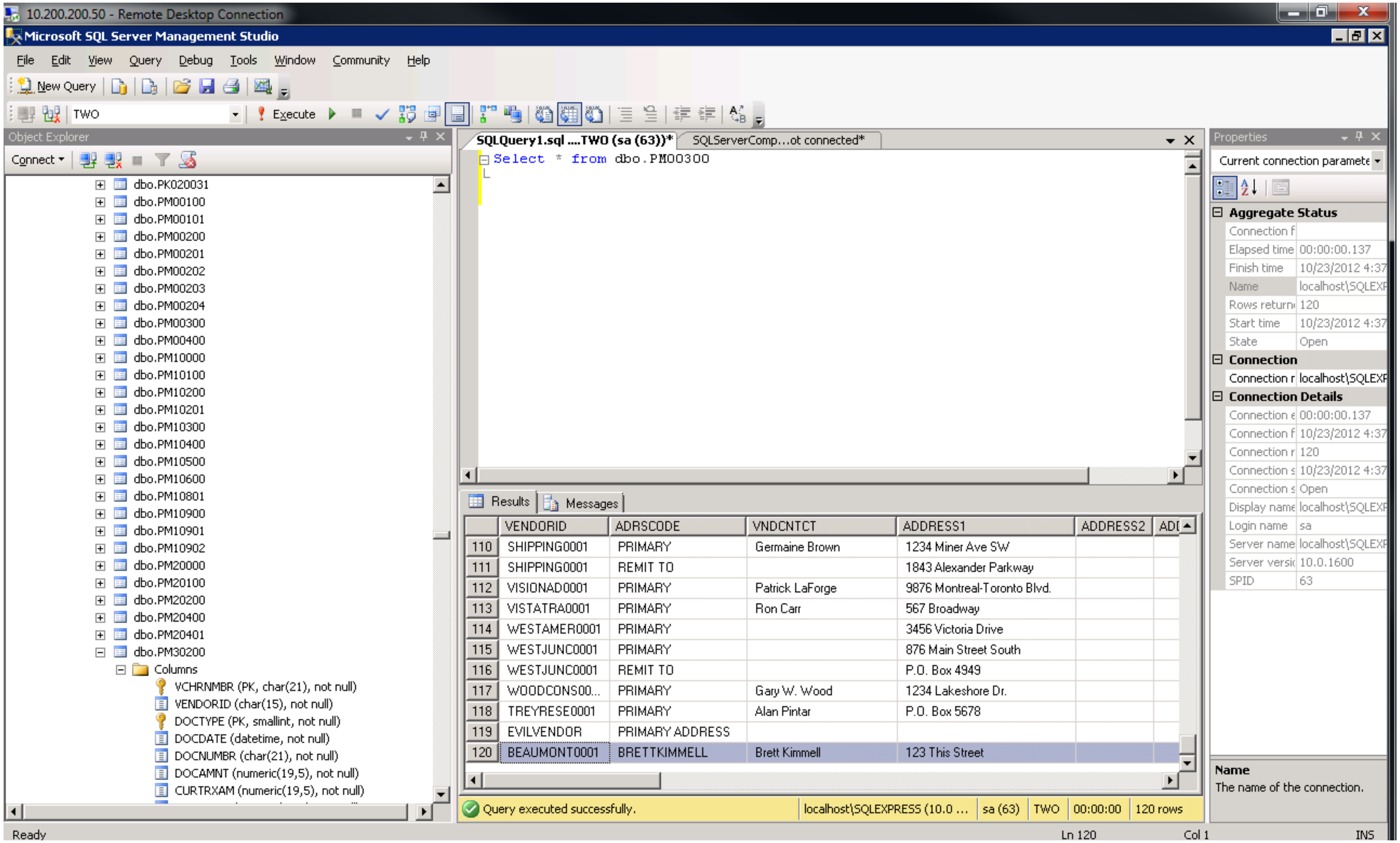
ts

```
,[VNDCNTCT]
,[ADDRESS1]
,[ADDRESS2]
,[ADDRESS3]
,[CITY]
```

	VENDORID	VENDNAME	VNDCHKNM	VENDSHNM	VADDC
1	ACETRAVE0001	A Travel Company	A Travel Company	A Travel	PRIMA
2	ADVANCED0001	Advanced Office Systems	Advanced Office Systems	Advanced Office	PRIMA
3	ALLENSON0001	Allenson Properties	USA-US-M	USA-US-M	PRIMA
4	AMERICAN0001	AmericaCharge	AmericaCharge	AmericaCharge	PRIMA
5	ATTRACTI00001	Attractive Telephone Co.	Attractive Telephone Co.	Attractive	PRIMA
6	ASSOCIAT0001	Associated Insurance Inc.	Associated Insurance Inc.	Associated Insu	PRIMA
7	AUSTRALIA	AUSTRALIA	AUSTRALIA	AUSTRALIA	
8	BEAUMONT0001	Beaumont Construction	Your Company Name Here!!	Beaumont Constr	PRIMA
9	BERGERON0001	Bergeron Communications Sol.	Bergeron Communications Sol.	Bergeron Commun	PRIMA

Query executed successfully. | localhost\SQLEXPRESS (10.0 ... | sa (52) | master

Manipulating Existing Vendor Records' Remit-To Address



10.200.200.50 - Remote Desktop Connection
Microsoft SQL Server Management Studio
File Edit View Query Debug Tools Window Community Help
New Query
TWO
Execute
Object Explorer
Connect
SQLQuery1.sql ....TWO (sa (63))*
SQLServerComp....ot connected*
Properties
Current connection paramete
Results
Messages

```
Select * from dbo.PM00300
```

dbo.PK020031
dbo.PM00100
dbo.PM00101
dbo.PM00200
dbo.PM00201
dbo.PM00202
dbo.PM00203
dbo.PM00204
dbo.PM00300
dbo.PM00400
dbo.PM10000
dbo.PM10100
dbo.PM10200
dbo.PM10201
dbo.PM10300
dbo.PM10400
dbo.PM10500
dbo.PM10600
dbo.PM10801
dbo.PM10900
dbo.PM10901
dbo.PM10902
dbo.PM20000
dbo.PM20100
dbo.PM20200
dbo.PM20400
dbo.PM20401
dbo.PM30200
Columns
VCHRNMBR (PK, char(21), not null)
VENDORID (char(15), not null)
DOCTYPE (PK, smallint, not null)
DOCDATE (datetime, not null)
DOCNUMBR (char(21), not null)
DOCAMNT (numeric(19,5), not null)
CURTRXAM (numeric(19,5), not null)

	VENDORID	ADRSCODE	VNDCNTCT	ADDRESS1	ADDRESS2	ADI
110	SHIPPING0001	PRIMARY	Germaine Brown	1234 Miner Ave SW		
111	SHIPPING0001	REMIT TO		1843 Alexander Parkway		
112	VISIONAD0001	PRIMARY	Patrick LaForge	9876 Montreal-Toronto Blvd.		
113	VISTATRA0001	PRIMARY	Ron Carr	567 Broadway		
114	WESTAMER0001	PRIMARY		3456 Victoria Drive		
115	WESTJUNC0001	PRIMARY		876 Main Street South		
116	WESTJUNC0001	REMIT TO		P.O. Box 4949		
117	WOODCONS00...	PRIMARY	Gary W. Wood	1234 Lakeshore Dr.		
118	TREYRESE0001	PRIMARY	Alan Pintar	P.O. Box 5678		
119	EVILVENDOR	PRIMARY ADDRESS				
120	BEAUMONT0001	BRETTKIMMELL	Brett Kimmell	123 This Street		

Query executed successfully. | localhost\SQLEXPRESS (10.0 ... | sa (63) | TWO | 00:00:00 | 120 rows

Ready | Ln 120 | Col 1 | INS

Aggregate Status

Connection f	
Elapsed time	00:00:00.137
Finish time	10/23/2012 4:37
Name	localhost\SQLEXP
Rows returni	120
Start time	10/23/2012 4:37
State	Open

Connection

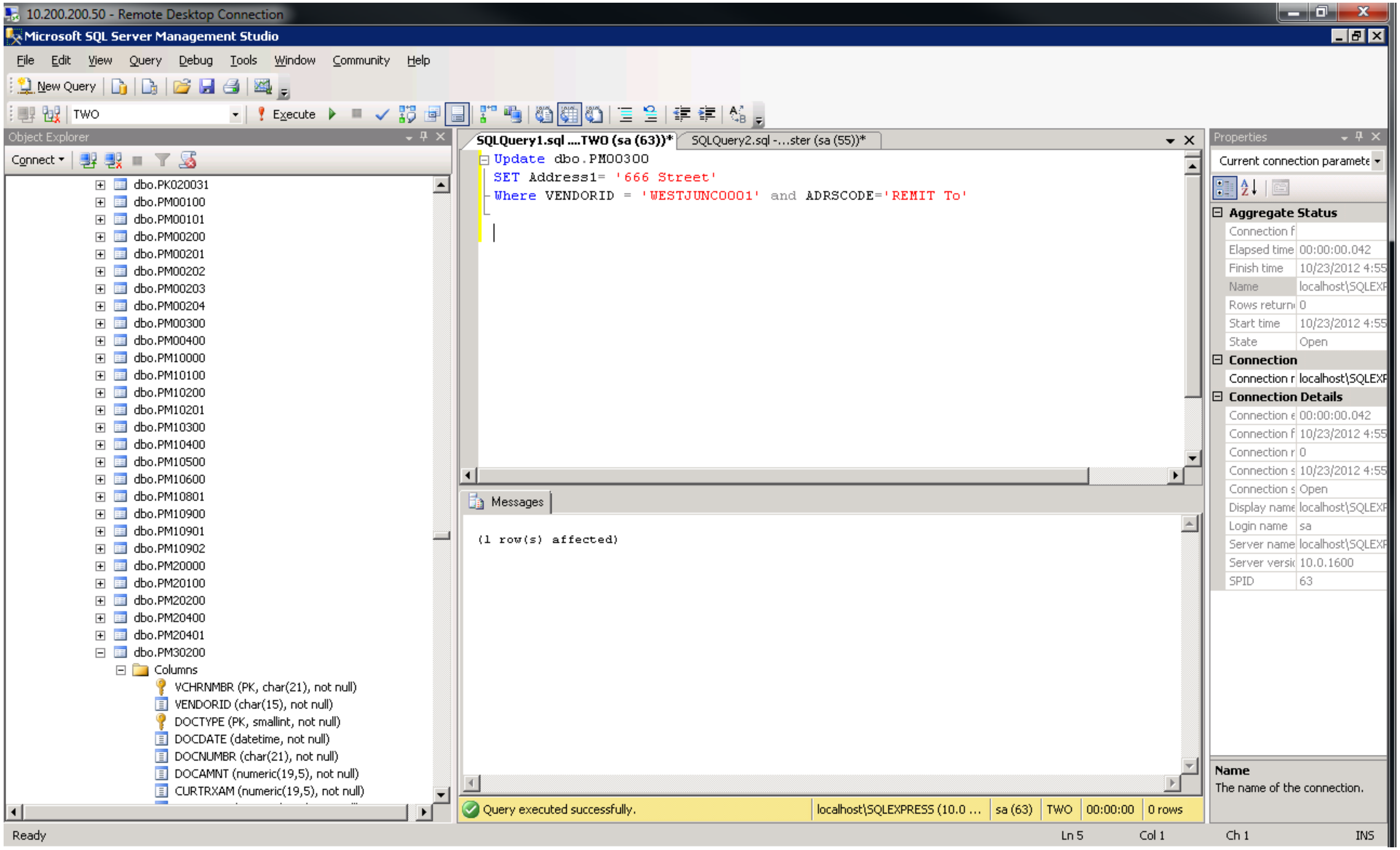
Connection r	localhost\SQLEXP

Connection Details

Connection e	00:00:00.137
Connection f	10/23/2012 4:37
Connection r	120
Connection s	10/23/2012 4:37
Connection s	Open
Display name	localhost\SQLEXP
Login name	sa
Server name	localhost\SQLEXP
Server versic	10.0.1600
SPID	63

Name
The name of the connection.

Remit-To cont……



SQLQuery1.sql ....TWO (sa (63))* | SQLQuery2.sql -…ster (sa (55))*

```
Update dbo.PM00300
SET Address1= '666 Street'
Where VENDORID = 'WESTJUNC0001' and ADRSCODE='REMIT To'
```

```
(1 row(s) affected)
```

Query executed successfully. | localhost\SQLEXPRESS (10.0 ... | sa (63) | TWO | 00:00:00 | 0 rows

Ln 5 Col 1 Ch 1 INS

Object Explorer:

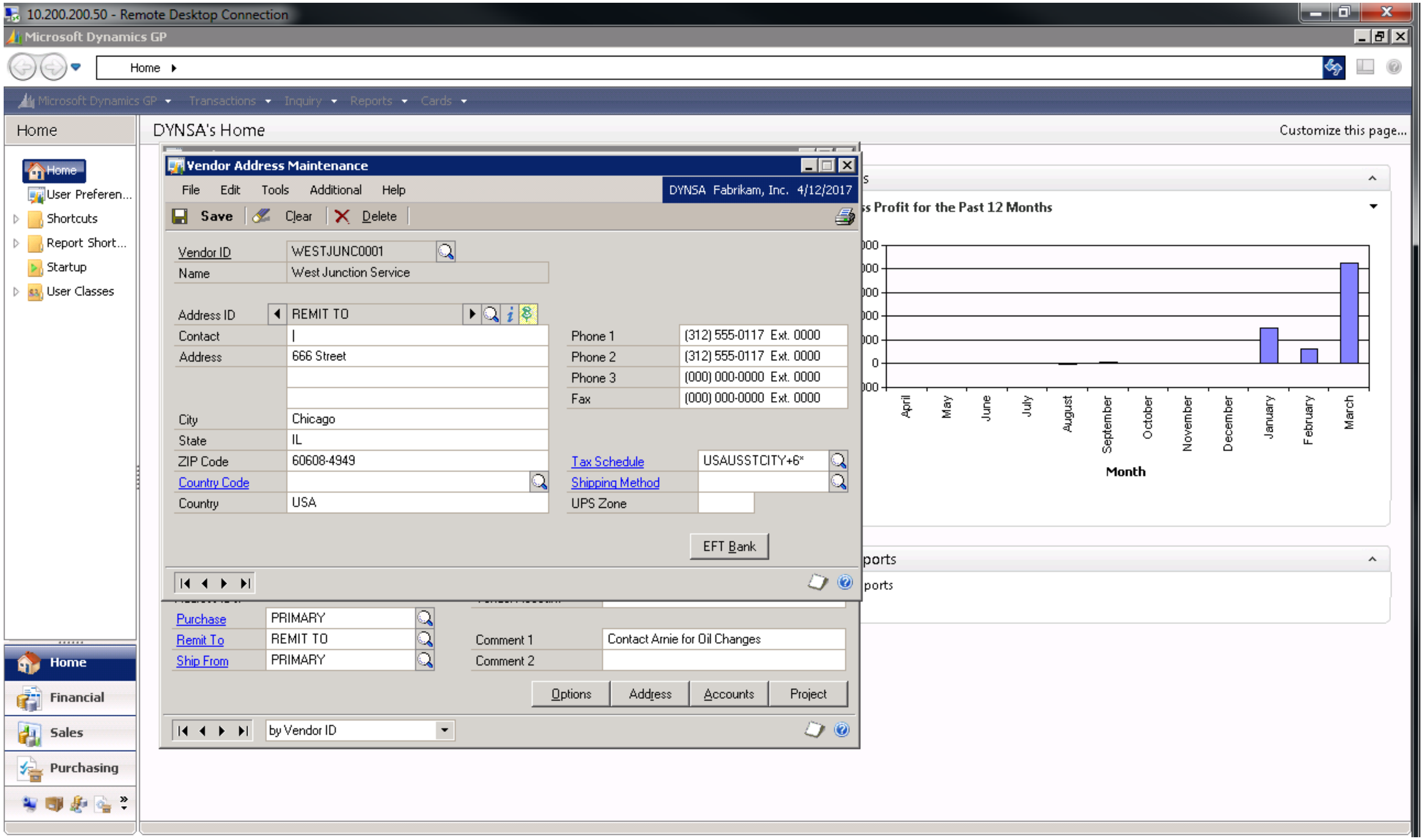
- dbo.PK020031
- dbo.PM00100
- dbo.PM00101
- dbo.PM00200
- dbo.PM00201
- dbo.PM00202
- dbo.PM00203
- dbo.PM00204
- dbo.PM00300
- dbo.PM00400
- dbo.PM10000
- dbo.PM10100
- dbo.PM10200
- dbo.PM10201
- dbo.PM10300
- dbo.PM10400
- dbo.PM10500
- dbo.PM10600
- dbo.PM10801
- dbo.PM10900
- dbo.PM10901
- dbo.PM10902
- dbo.PM20000
- dbo.PM20100
- dbo.PM20200
- dbo.PM20400
- dbo.PM20401
- dbo.PM30200
  - Columns
    - VCHRNMBR (PK, char(21), not null)
    - VENDORID (char(15), not null)
    - DOCTYPE (PK, smallint, not null)
    - DOCDATE (datetime, not null)
    - DOCNUMBR (char(21), not null)
    - DOCAMNT (numeric(19,5), not null)
    - CURTRXAM (numeric(19,5), not null)

Properties: Current connection paramete

Aggregate Status	
Connection f	
Elapsed time	00:00:00.042
Finish time	10/23/2012 4:55
Name	localhost\SQLEXF
Rows return	0
Start time	10/23/2012 4:55
State	Open
Connection	
Connection r	localhost\SQLEXF
Connection Details	
Connection e	00:00:00.042
Connection f	10/23/2012 4:55
Connection r	0
Connection s	10/23/2012 4:55
Connection s	Open
Display name	localhost\SQLEXF
Login name	sa
Server name	localhost\SQLEXF
Server versi	10.0.1600
SPID	63

Name
The name of the connection.

Remit-To cont……



Vendor Address Maintenance

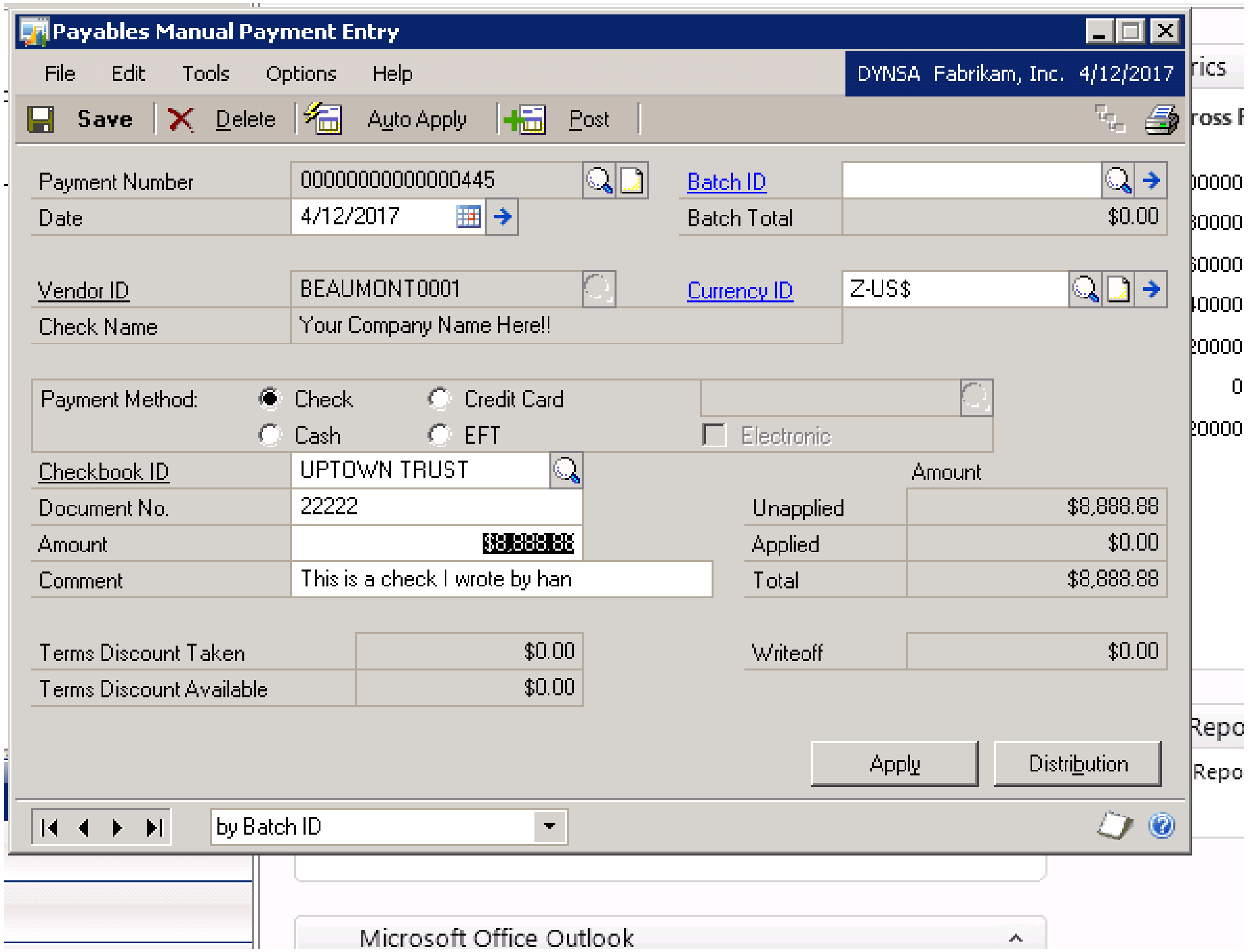
DYNSA Fabrikam, Inc. 4/12/2017

Vendor ID	WESTJUNC0001		
Name	West Junction Service		
Address ID	REMIT TO		
Contact		Phone 1	(312) 555-0117 Ext. 0000
Address	666 Street	Phone 2	(312) 555-0117 Ext. 0000
		Phone 3	(000) 000-0000 Ext. 0000
		Fax	(000) 000-0000 Ext. 0000
City	Chicago		
State	IL		
ZIP Code	60608-4949	Tax Schedule	USAUSSTCITY+6*
Country Code		Shipping Method	
Country	USA	UPS Zone	

Purchase	PRIMARY		
Remit To	REMIT TO	Comment 1	Contact Arnie for Oil Changes
Ship From	PRIMARY	Comment 2	

by Vendor ID

Create a New Vendor and Manual Check Entry (Mayhem PoC)



DYNSA Fabrikam, Inc. 4/12/2017

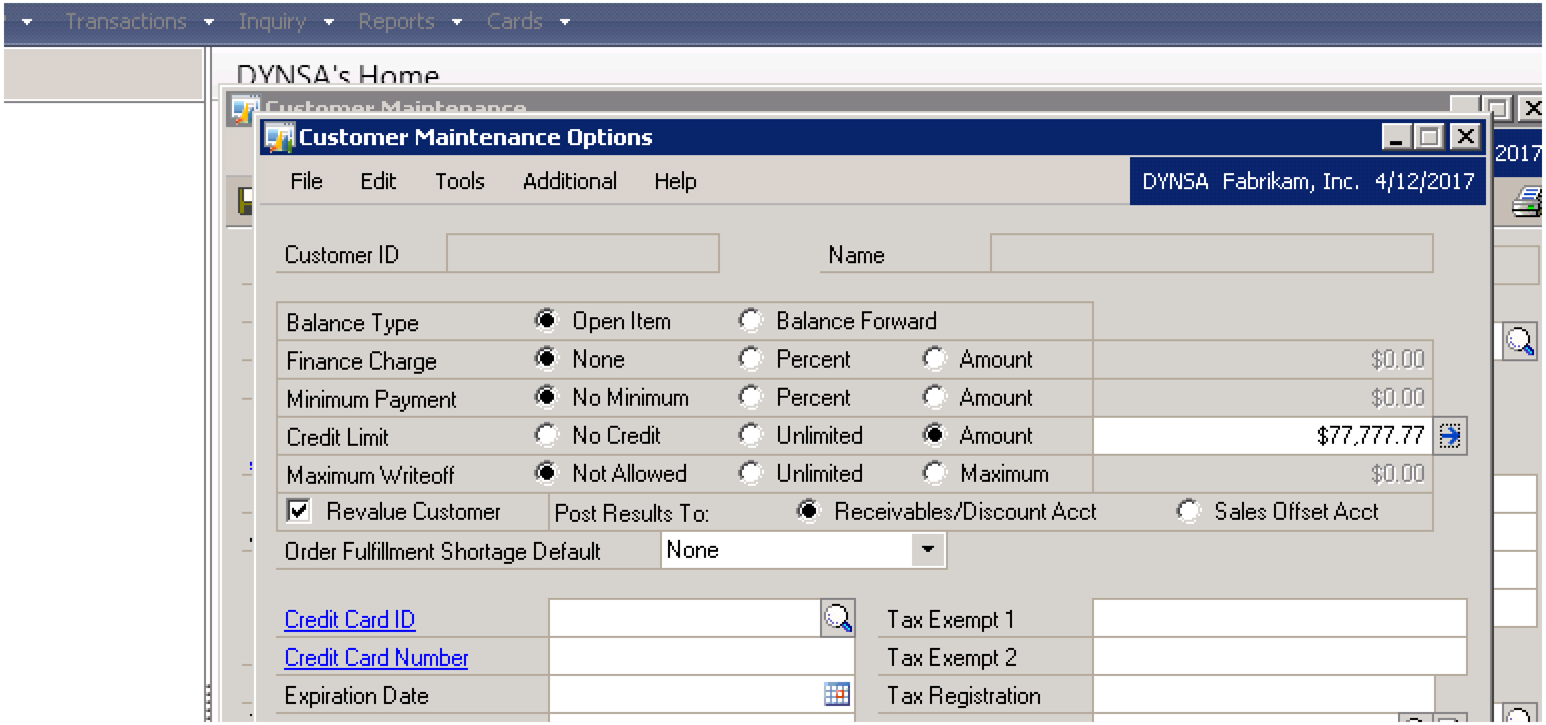
Payment Number	00000000000000445	Batch ID	
Date	4/12/2017	Batch Total	$0.00
Vendor ID	BEAUMONT0001	Currency ID	Z-US$
Check Name	Your Company Name Here!!		

Payment Method: ● Check ○ Credit Card ○ Cash ○ EFT □ Electronic

Checkbook ID	UPTOWN TRUST		Amount
Document No.	22222	Unapplied	$8,888.88
Amount	$8,888.88	Applied	$0.00
Comment	This is a check I wrote by han	Total	$8,888.88
Terms Discount Taken	$0.00	Writeoff	$0.00
Terms Discount Available	$0.00		

by Batch ID

Increase Customer Credit Limit



Customer ID

Name

Balance Type	● Open Item	○ Balance Forward		
Finance Charge	● None	○ Percent	○ Amount	$0.00
Minimum Payment	● No Minimum	○ Percent	○ Amount	$0.00
Credit Limit	○ No Credit	○ Unlimited	● Amount	$77,777.77
Maximum Writeoff	● Not Allowed	○ Unlimited	○ Maximum	$0.00

☑ Revalue Customer Post Results To: ● Receivables/Discount Acct ○ Sales Offset Acct

Order Fulfillment Shortage Default: None

Credit Card ID

Credit Card Number

Expiration Date

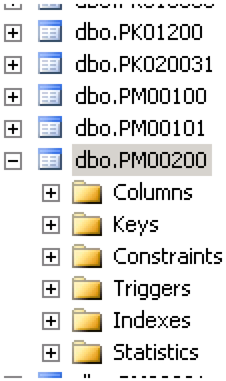
Tax Exempt 1

Tax Exempt 2

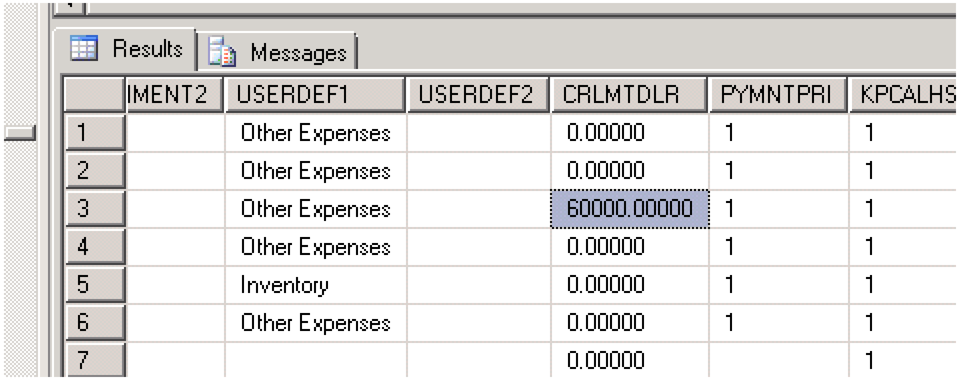
Tax Registration

Increase Customer Credit Limit

CREDTLMT (Credit Limit) in PM00200: (Thanks to Bud Cool, a frequent contributor to the Microsoft GP Newsgroup, for this information!) 0 – No Credit, 1 – Unlimited, 2 – Amount. Note: If CREDTLMT = 2 then CRLMTDLR contains the amount of the credit limit, otherwise CRLMTDLR is zero.

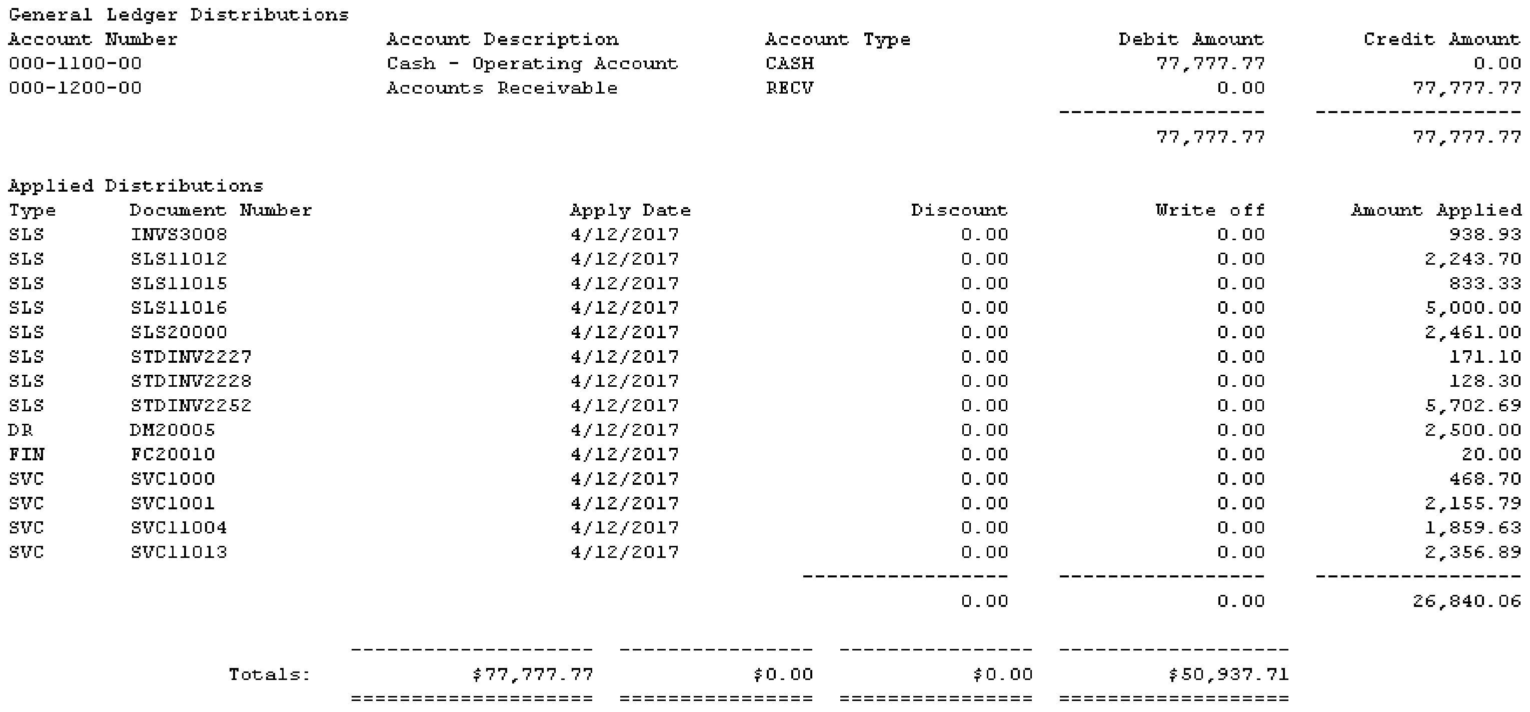


- dbo.PK01200
- dbo.PK020031
- dbo.PM00100
- dbo.PM00101
- dbo.PM00200
  - Columns
  - Keys
  - Constraints
  - Triggers
  - Indexes
  - Statistics



	IMENT2	USERDEF1	USERDEF2	CRLMTDLR	PYMNTPRI	KPCALHS
1		Other Expenses		0.00000	1	1
2		Other Expenses		0.00000	1	1
3		Other Expenses		60000.00000	1	1
4		Other Expenses		0.00000	1	1
5		Inventory		0.00000	1	1
6		Other Expenses		0.00000	1	1
7				0.00000		1

Credit Balance in Customer Account, Get a Refund



```
General Ledger Distributions
Account Number               Account Description          Account Type                  Debit Amount          Credit Amount
000-1100-00                  Cash - Operating Account     CASH                             77,777.77                   0.00
000-1200-00                  Accounts Receivable          RECV                                  0.00              77,777.77
                                                                                   -----------------      -----------------
                                                                                           77,777.77              77,777.77

Applied Distributions
Type      Document Number                   Apply Date                Discount            Write off         Amount Applied
SLS       INVS3008                          4/12/2017                     0.00                 0.00                 938.93
SLS       SLS11012                          4/12/2017                     0.00                 0.00               2,243.70
SLS       SLS11015                          4/12/2017                     0.00                 0.00                 833.33
SLS       SLS11016                          4/12/2017                     0.00                 0.00               5,000.00
SLS       SLS20000                          4/12/2017                     0.00                 0.00               2,461.00
SLS       STDINV2227                        4/12/2017                     0.00                 0.00                 171.10
SLS       STDINV2228                        4/12/2017                     0.00                 0.00                 128.30
SLS       STDINV2252                        4/12/2017                     0.00                 0.00               5,702.69
DR        DM20005                           4/12/2017                     0.00                 0.00               2,500.00
FIN       FC20010                           4/12/2017                     0.00                 0.00                  20.00
SVC       SVC1000                           4/12/2017                     0.00                 0.00                 468.70
SVC       SVC1001                           4/12/2017                     0.00                 0.00               2,155.79
SVC       SVC11004                          4/12/2017                     0.00                 0.00               1,859.63
SVC       SVC11013                          4/12/2017                     0.00                 0.00               2,356.89
                                                                 -----------------    -----------------      -----------------
                                                                              0.00                 0.00              26,840.06

                            --------------------  ----------------  ----------------  -------------------
                  Totals:             $77,777.77             $0.00             $0.00           $50,937.71
                            ====================  ================  ================  ===================
```

Other Fraud Attacks

- Mass Steal Banking Information
- Mass Steal Credit Card Data
- Private Financial Records

Accounting Controls to Prevent Fraud

Bank Reconciliation

- Timing is everything
- Bank reconciliation compares the bank balance with the book balance monthly

Accounting Controls

- Matching Checks Cut to Invoices
- Matching Address on Check to Address on Invoice
- Process for Adding Vendors to System
- Customer On-Boarding Process
- Confirmation of Vendor Banking Information
- Account Reconciliations

Conclusions

What about Technical Controls?

- Never discount “Defense-in-Depth”
- All it takes is for one control to fail!
  - GP, SQL server, user permissions/roles, security awareness, antivirus, IDS, incident response
- This is why the accounting controls are more important to implement

Final Thoughts

- It is possible to perpetrate fraud against the accounting system from the outside
- Fraud is much easier for an insider
- Combine malware with legitimate entries = perfect crime
- Combination of technical and accounting controls are required to combat modern fraud

Questions?

- **Tom Eston**
  teston@securestate.com
  Twitter: agent0x0
  Blog: Spylogic.net

- **Brett Kimmell**
  bkimmell@securestate.com
  Twitter: kimmellbrett

- More details on attacks included in our whitepaper