



Third Party Payment Processors: Relationships, Guidance, and Case Examples

Michael Benardo

*Chief, Cyber-Fraud and Financial Crimes Section
Federal Deposit Insurance Corporation
Washington, D.C.*

Joel Sweet

Trial Attorney

*U.S. Department of Justice; Consumer Protection Branch
Washington, D.C.*

Jennifer LaRoche

Special Counsel

*Office of the Comptroller of the Currency
Washington, D.C.*

Michael B. Benardo

Chief, Cyber Fraud and Financial Crimes Section
Federal Deposit Insurance Corporation
Washington, DC
mbenardo@fdic.gov

Michael B. Benardo is the Chief of the Cyber Fraud and Financial Crimes Section in the FDIC's Division of Supervision and Consumer Protection. He oversees all aspects of fraud-related initiatives, including establishment of regulatory policies and procedures. He is instrumental developing and implementing fraud-related supervisory programs including examination techniques, and represents the FDIC on interagency working groups with a goal of developing consistent interagency programs for combating financial institution fraud.

Mr. Benardo has nineteen years of progressive experience with the FDIC, including serving as a Manager in the Technology Supervision Branch. He also served as a key member of the FDIC's Year 2000 project team from 1997 through the century date change.

Prior to his employment with the FDIC, Mr. Benardo spent six years working in the commercial banking industry. He worked in a variety of areas including several assignments in bank operations.

Mr. Benardo is a graduate of the University of South Florida with a B. S. degree in Finance.

Joel M. Sweet
Trail Attorney
U.S. Department of Justice, Consumer Protection Branch

Joel M. Sweet, a Trail Attorney for the U.S. Department of Justice; Consumer Protection Branch, was the lead prosecutor in United States v. Payment Processing Center, LLC, C.A. 06-725 (E.D. Pa.), in which the government shut down a third-party payment processor, seized the assets of the company and its principals, and litigated with Wachovia Bank concerning its business relationship with the payment processor. That action led to an investigation and enforcement action by the Office of the Comptroller of the Currency, a private class action alleging racketeering by Wachovia Bank, and the implementation of a \$150 million victim restitution program.

In addition to consumer fraud, Mr. Sweet prosecutes cases involving healthcare and defense contract fraud, and also defends the government in a variety of civil matters. Mr. Sweet consults regularly with the Federal Reserve Board, the Federal Trade Commission, and state Attorneys General, concerning payment systems abuse and consumer fraud. He is a member of the Department of Justice's Mass-Marketing Fraud Working Group.

Before joining government, Mr. Sweet was a commercial litigator specialization in business disputes, class action litigation, and securities fraud. Mr. Sweet was a member of the Plaintiffs' Counsel Executive Committee in In re Holocaust Victim Assets Litigation, C.A. No. 4849 (E.D.N.Y.), a class action against Switzerland's three largest banks that settled in 1998 for \$1.25 billion.

Jennifer LaRoche is an Attorney in the Enforcement and Compliance Division since September 1999. As an attorney in the E&C Division, she has worked extensively on issues involving credit card banks and predatory and abusive lending. T Bank was her first payment processor case. Jennifer Graduated from University of Maryland Law School in 1999.

Third Party Payment Processor Relationships

September 17, 2013

Michael B. Benardo
Chief, Cyber Fraud & Financial Crimes Section
Division of Risk Management Supervision
Federal Deposit Insurance Corporation



Third Party Payment Processors

- TPPPs: What they are?
 - A deposit customer that uses its banking relationship to process payments for merchant clients

- Merchant Clients
 - Legitimate?
 - High Risk
 - Illegal

High Risk Merchants/Activities

- Ammunition Sales
- "As Seen on TV"
- Credit Card Schemes
- Credit Repair Services
- Drug Paraphernalia
- Escort Services
- Firearms/Fireworks Sales
- Gambling
- Get Rich Products
- Government Grants
- Home Based Charities
- Life Time Guarantees
- Pyramid Type Sales
- Pay Day Loans
- Pharmaceutical Sales
- Pornography
- Ponzi Schemes
- Racist materials
- Raffles/Sweepstakes
- Surveillance equipment
- Telemarketing
- Tobacco Sales
- Other Payment Processors

Typical Payment Types

- Remotely Created Checks (RCC)/Demand Drafts
- Automated Clearing House (ACH)

Remotely Created Check

THIS CHECK IS VOID WITHOUT A BURGUNDY BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK - HOLD AT ANGLE TO VIEW

Payment Processing Center
1262 Wood Lane, Suite 103
Langhorne, PA 19047
1-866-223-8711

BANKNORTH MASSACHUSETTS
BREWSTER, MA 02631
53-7054/2113

Check #: 229554

Date: 05/05/05

Pay to the order of: Call One Communications 800-357-8873

** 149.90 **

One Hundred Fourty Nine Dollars and Ninety Cents *****

Wilson [REDACTED]
[REDACTED]
Worcester, MA 01604
For Customer Service Call (800) 357-8873
05052005-225.csv

Authorized By Your Depositor
No Signature Required
Reference # 11007157

IN SIGNATURE HAS A COLORED BACKGROUND - BORDERS CONTAINING MICROPRINTING

229554

0000014990#

Warning Signs/Red Flags

- Consumer Complaints (i.e., unauthorized, misrepresented, merchant strong-armed consumer into providing account information)
- High rates of unauthorized returns/charge backs
- TPPPs have been targeting problem institutions with the promise of income and capital
- TPPP likely to use more than one financial institution to process payments and activity may periodically move between financial institutions

Enhanced Due Diligence

- Policies and procedures
- Know Your TPPPs customers
- Develop a processor approval program that extends beyond credit risk management
- Perform background checks on TPPPs and merchant clients
- Authenticate the TPPPs business operations and assess the risk level

Enhanced Due Diligence (Continued)

- Review promotional materials, including Websites, to determine target clientele
- Identify processor's major customers
- Review corporate documentation
- Visit business operation center
- Review information of merchant clients; the principle business activity; geographic location; and sales techniques

Ongoing Monitoring Systems

- Monitoring high rates of return
- Setting return rate thresholds
- Setting transaction volume limits
- Auditing third party processors program
- Monitoring reserve adequacy
- Monitoring consumer complaints about merchant clients on Internet blogs and industry databases
- Developing contract language addressing access to records, conditions requiring account closing, and reserve adequacy

Potential Supervisory Responses

May require the bank to terminate the relationship with the high-risk TPPP

- Informal enforcement actions
- Formal enforcement actions
- Civil Money Penalties
- Section 5 of the FTC Act

Unfair or Deceptive Practices?

- A bank may be viewed as facilitating a TPPP's or a merchant's fraudulent or unlawful activity
- Section 5(a) of the FTC Act prohibits “unfair or deceptive acts or practices affecting commerce” and applies to all persons engaged in commerce, including banks
- Authority under section 8 of the FDI Act to take appropriate action when unfair or deceptive acts or practices are discovered

When a Bank Suspects Fraudulent Activity

- File a Suspicious Activity Report
- Require the TPPP to cease processing for that specific merchant
- Terminate the relationship with the TPPP

Resources

- FDIC Revised Guidance on Payment Processor Relationships (FIL-3-2012), dated January 31, 2012 (FDIC Guidance was first issued in 2008 (FIL-127-2008) but was updated in 2012)
- FinCEN Advisory on Risks Associated with Third-Party Payment Processors (FIN-2012-A010), dated October 22, 2012
- Supervisory Insights – Summer 2011

Resources (Continued)

- FDIC Guidance for Managing Third-Party Risk (FIL-44-2008), dated June 6, 2008
- OCC Bulletin on Payment Processors (OCC-2008-12), dated April 24, 2008
- FFIEC Handbook on Retail Payment Systems (March 2004) – Coverage of ACH Activities
- 2010 FFIEC BSA/AML Examination Manual



Comptroller of the Currency
Administrator of National Banks

Payment Processors: Guidance for Examiners & Fraud Specialists

Jennifer J. LaRoche
Special Counsel, Enforcement & Compliance
Office of the Comptroller of the Currency
Jennifer.LaRoche@occ.treas.gov
202-649-6200

Disclaimer

The views and opinions expressed in this presentation are my own and do not necessarily reflect the views of the OCC or any other government agency or official.



OCC Bulletin 2008-12

Risk Management Guidance for Payment Processor Accounts

- Heightened risks
- Appropriate due diligence on processors and their clients
- Effective underwriting
- Ongoing account monitoring, including of return volumes
- Banks without proper controls may be viewed as facilitating underlying fraud
- Take immediate action upon identifying improper activity (i.e., file SAR, terminate relationship)
- Additional guidance: OCC Bulletins 2006-39, 2006-13, 2001-47, Comptroller's Handbook, FFIEC BSA/AML Exam Manual and FDIC FIL 3-2012 and FIL-127-2008



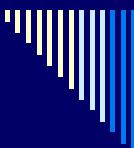
Risk Mitigation Practices

- Abide by all applicable guidance, laws and regulations
- Understand the risks and have appropriate controls, policies and procedures
- Know your customer, and your customer's customers
- Monitor account activity, particularly returns
- Investigate complaints and fraud warnings
- Validate information provided by the processor
- Obtain collateral and institute a debit restraint
- Be aware of current scams and schemes
- Act immediately upon identifying suspicious activity



Examining Guidance

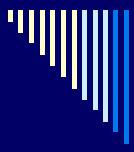
- Verify the bank's due diligence and underwriting
- Review the bank's controls, policies and procedures for high-risk accounts
- If you find suspicious activity:
 - Gather information to support your findings
 - Escalate your findings to your supervisors
 - Communicate to the bank the seriousness of potentially facilitating consumer fraud
 - Encourage the bank to file a SAR and to contact law enforcement



Red Flags

- High return rates
- Merchants selling questionable products and services
- 100% refund policy
- Prior civil, criminal and regulatory actions against processor or its principals
- Consumer and other bank complaints
- Inquiries from law enforcement





If there are internet merchants, watch for the following:

- Reliance by bank on real time transaction details obtained from the merchant.
- Merchants who market via pop-ups on websites.



Notice of Affidavit received.

Bank Name
Address

RE: Affidavit for Account Number and Check 9999
Affidavit received on 02/22/07 for Customer Name

Dear Bank,

Your account holder has submitted an affidavit stating that the above mentioned item that was drafted against their account was not authorized.

We dispute this claim on the basis that this was a transaction that was generated in a secure area on our customer's website that required your account holder to agree to the terms and conditions and provide the information necessary to create an electronic draft. We have confirmed the information showing that your customer was on www.xyz.org when he opted to purchase the service offered by www.abc.com. His IP address was captured as well as the name of the internet provider he currently uses. If your customer would like a copy of the information or would like a refund, please have them go to www.abc.com complete the customer service form and someone will contact her immediately. Your assistance is greatly appreciated.

Sincerely

VP
T Bank
Telephone number
E-mail Address

Real-Time Checks Transactions Details

Transaction ID	212765
Timestamp	11/27/2006 4:07:34 PM
Customer ID (old)	0
Order ID (old)	0
Customer ID	65.4.146.169:www.xyz.org:1469
Order ID	rage13 dbl@yahoo.cor
Name On Check	Customer Name
Address Line 1	Customer's Street Address
Address Line 2	
Address Line 3	Customer's city, state
Name of Bank	Bank Name
Bank Address Line 1	

Real-Time Checks Transactions Details Continued

Bank Address Line 2	
Routing Number	Routing Number
Account Number	Account Number
Check Number	9999
Amount	\$49.45
Error	<input type="checkbox"/>
Passed	<input checked="" type="checkbox"/>
Details	pass
Batch ID	4925
Check ID	354847

Special bonus of
Check out these offers and click the button below

Get a FREE Auto Loan Quote

Yes No



I want an auto loan to buy just the car I need.

[View Details](#) [Privacy Policy](#) [Terms and Conditions](#)

Get a \$2,500 MasterCard

Yes No



I want a \$2,500 prepaid debit Mastercard with no credit check required!

[View Details](#) [Privacy Policy](#) [Terms and Conditions](#)

Finish matching me with offers

© 2007 GeniebyName.com

BSA/AML Risks

- 31 U.S.C. §§ 5311 et seq. & 31 C.F.R. Part 103
- T Bank Consent Order
- Upstate National Bank Consent Order
- Need for enhanced BSA/AML program
that can identify, monitor and address the
greater than normal risk posed by payment
processor relationships





Legal Basis for Enforcement Actions

- Recklessly engaged in unsafe or unsound banking practices
- Engaged in unfair practices in violation of Section 5 of the FTC Act
- Banks directly liable because “but for” the banks the TPPP and their merchant-clients would not have had access to the payments system



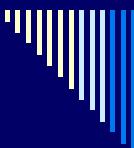
OCC v. Wachovia

- OCC Formal Investigation
- Wachovia-PPC relationship



Wachovia-PPC Relationship

- PPC accounts opened at Wachovia in Philadelphia
- High returns projected
- PPC assurances
 - Strict controls over telemarketers
 - 100% refund policy for consumers who complained
 - Telemarketer calls monitored and recorded
- Deposits began in March 2005
- 1.8 million RCCs totaling \$142 million
- 950,000 RCCs returned generating \$1.45 million in return item fees for Wachovia



OCC v. T Bank

- Giact-referred merchants opened accounts at T Bank into which they deposited RCCs
 - 13 of these merchants engaged in fraud or deceptive practices; some were telemarketers and others were internet merchants
 - First of the 13 merchants opened an account in June 2006
 - At OCC direction, Bank terminated all Giact-related accounts in August 2007
- Genesis--Routine safety and soundness exam found:
 - high return rates
 - inadequate due diligence
 - Lack of monitoring of return rates and reasons for returns
- OCC Formal Investigation

T Bank-Giact Relationship

- Bank focused on the fee income generated by returns
- \$22.6 million in RCCs deposited into the 13 merchants' accounts
- \$16.6 million of this amount was returned
- \$1.95 million in return fees for T Bank

Fraud Warnings at T Bank

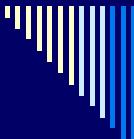
- Return rate of over 50%
- High volume of returns as unauthorized, fraud, NSF, and account closed
- Consumer complaints
- Complaints from other financial institutions
- Internal Warnings
- Law Enforcement Inquiries/State AG Complaints or Injunctions
- Types of merchants (check FTC website)
 - merchant finance cards;
 - prepaid debit cards;
 - credit repair companies;
 - travel discount clubs; and
 - telemarketing services/call fulfillment companies





What Went Wrong at Both Wachovia and T Bank

- Inadequate due diligence and underwriting
- Poor risk recognition and response
- Weak controls, policies and procedures
- Inadequate account monitoring
- Inadequate case management tools
- Failure to heed consumer complaints



What Went Wrong at Both Wachovia and T Bank (Continued)

- Policy exception instituted to handle PPC returns
- Poor coordination of internal investigations
- Lack of follow-up on law enforcement inquiries
- Relied on Giact to conduct due diligence on the merchants
- Failure to consider Giact's AML practices
- Ignored information contained in due diligence reports conducted by its outside counsel



Comptroller's Findings in Both Wachovia and T Bank

- Unsafe or unsound banking practices
- Unfair practices in violation of Section 5 of the FTC Act
- Consumers harmed



Enforcement Actions

- Wachovia
 - Over \$150 million in restitution to 740,000 consumers
 - \$10 million civil money penalty
 - \$8.9 million contribution to consumer education
 - Corrective action
- T Bank
 - \$5.3 million in restitution to 55,997 consumers
 - \$100,000 civil money penalty
 - Corrective action—both a BSA Consent Order and a Consent Order requiring policies, procedures, and controls should the Bank enter into a relationship with an entity that deposits RCCs.

United States of America

v.

Payment Processing Center

A Case Study of Remotely Created Check Abuse and Payment System Vulnerabilities

Joel M. Sweet, Trial Attorney, Consumer Protection Branch, DOJ
(detailee from United States Attorney's Office for the Eastern District of Pennsylvania)

1

Disclaimer

Any opinions reflected in this presentation are those of the presenter and are not necessarily those of the Department of Justice, or any government official, agency, department, or branch.

The information in this presentation is from public sources.

2

Mass Market Consumer Fraud – a National Scourge

Bernie Madoff swindled more than \$40B from a select group of mostly wealthy investors.



Fraudsters steal more than \$40B from consumers – mostly the elderly and those in the lower middle class – every year!

Which is most likely to receive attention from law enforcement, regulators, and the press: a single theft of \$100 million, or one million thefts of \$100?

3

Common Methods of Payment System Abuse

- Debit transactions originated by payment processors and banks on behalf of telemarketing and Internet fraudsters
- Phone company bills used to originate unauthorized charges (“cramming”)
- Mortgage payment mechanisms used to originate unauthorized charges

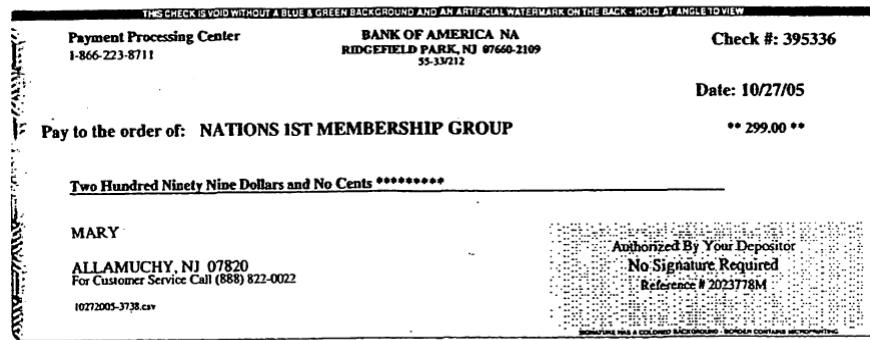
4

Law Enforcement Challenges to Prosecuting Telemarketing/Internet Fraud

- Jurisdictional limitations (state and international)
- Fraudsters change corporate identities and law enforcement plays “whack-a-mole”
- Victims are dispersed geographically
- Victims cannot identify fraudsters – no face-to-face contact
- Plausible deniability – cross-pointing among call centers, mail houses, fulfillment centers, payment processors, and banks
- Limited investigative and prosecutorial resources
- Limited reach of State Attorneys General and FTC

5

A Remotely Created Check (“RCC”)



6

RCC Fraud: Well-Known to Banks

“Demand drafts can be misused to commit check fraud. This practice involves the misuse of account information to obtain funds from a person’s bank account without that person’s signature on a negotiable instrument. . . **demand drafts have been used by deceptive telemarketers who obtain bank account information and withdraw unauthorized funds from consumers' bank accounts**, without their realizing that such withdrawals are occurring. . . .”

A Guide to Checks and Check Fraud, published by **Wachovia**, 2003

7

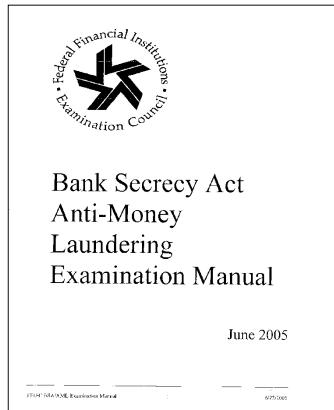
RCC Fraud: Well-Known to State Law Enforcement and FRB

- In 2005, 35 state attorneys general jointly request that the Federal Reserve ban RCCs from the payments system:
 - “demand drafts are frequently used to perpetrate fraud on consumers”
 - “such drafts should be eliminated” in favor of other forms of payment
 - If not eliminated, mandatory marking of RCCs and other measures to protect consumers

8

RCC Fraud: Well-Known to Bank Regulators

BSA/AML Examination Manual (FRB, FDIC, NCUA, OCC, and OTS)



9

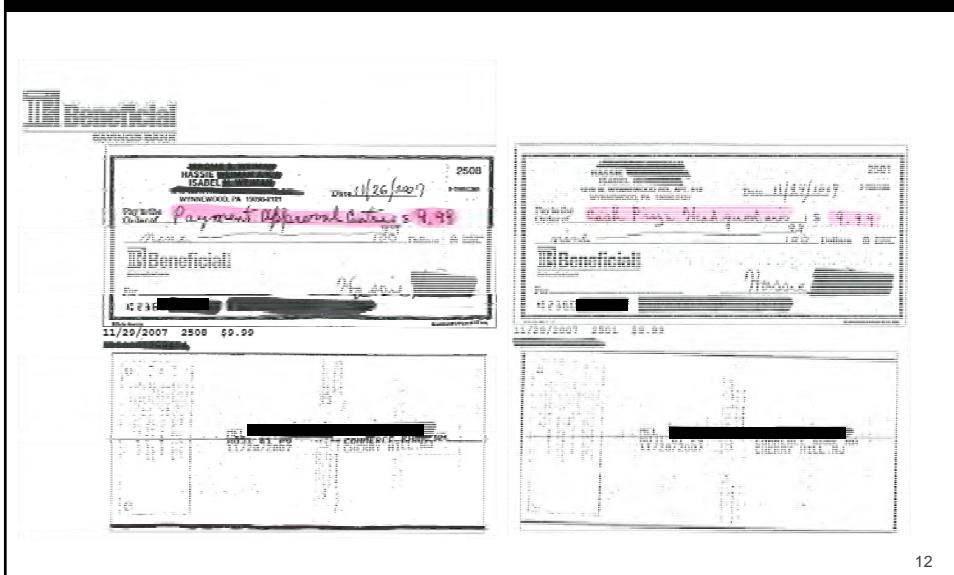
<p>BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL</p> <p>Expanded Overview – Third-Party Payment Processors</p> <p>OBJECTIVE</p> <p>Assess the adequacy of the bank's systems to manage the risks associated with its relationships with third-party payment processors, and management's ability to implement effective monitoring and reporting systems.</p> <p>OVERVIEW</p> <p>Non-bank, or third-party, payment processors (processors) are bank customers that provide payment processing services to merchants and other business entities.</p> <p>Traditionally, processors conducted primarily with retailers that had physical locations in order to process the retailers' transactions. These merchant transactions primarily included credit card payments but also covered automated clearing house demand drafts¹⁰⁹ (also known as e-checks), and debit and stored value card transactions. With the expansion of the Internet, retail borders have been eliminated. Processors may now service a variety of merchant accounts, including conventional retail and Internet-based establishments, prepaid travel, and Internet gaming enterprises.</p> <p>RISK FACTORS</p> <p>Processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, and fraud schemes.</p> <p>The bank's BSA/AML risks when dealing with a processor account are similar to risks from other activities in which the bank's customer conducts transactions through the bank on behalf of the customer's clients. When the bank is unable to accurately understand the nature and source of the transactions processed through an account, the risk to the bank and the likelihood of suspicious activity can increase. If a processor does not have an adequate processor approval program that goes beyond credit risk management, it could be vulnerable to processing illicit or criminal transactions.</p> <p><small>¹⁰⁹A demand draft is a substitute for a preprinted paper check. The draft is produced without a consumer signature but presumably with the consumer's authorization.</small></p>	<p>RISK MITIGATION</p> <p>Banks offering account services to processors should develop and maintain adequate policies, procedures, and processes to address risks related to these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level. Verification and assessment of a processor can be completed by performing the following procedures:</p> <ul style="list-style-type: none">Reviewing the processor's promotional materials, including its web site, to determine the target clientele. Businesses with elevated risk may include offshore companies, online gambling-related operations, and online payday lenders. For example, a processor whose customers are primarily offshore would be inherently riskier than a processor whose customers are primarily restaurants.Determining whether the processor re-sells its services to a third party who may be referred to as an "agent or provider of Independent Sales Organization (ISO) opportunities" or "gateway" arrangements.Reviewing the processor's policies, procedures, and processes to determine the adequacy of its due diligence standards for new merchants.Identifying the processor's major customers.Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.Visiting the processor's business operations center. <p>Banks that provide account services should monitor their processor relationships for any significant changes in the processors' business strategies that may affect their risk profile. Banks should periodically re-verify and update the processors' profiles to ensure the risk assessment is appropriate.</p> <p>In addition to adequate and effective account opening and due diligence procedures for processor accounts, management should monitor these relationships for unusual and suspicious activities. To effectively manage these accounts, the bank should have an understanding of the following processes, at a minimum:</p> <ul style="list-style-type: none">Merchant base.Merchant activities.Average number of dollar volume and number of transactions."Swapping" versus "keying" volume for credit card transactions.Charge-back history. <p><small>¹¹⁰Gateway arrangements are similar to an Internet service provider with excess computer storage capacity who sells its capacity to a third party, who would then offer computer services to various other individual businesses to the provider. The third party would be making decisions about who would be receiving the service, although the provider would be providing the ultimate storage capacity. Thus, the provider bears all of the risks while receiving a smaller profit.</small></p>				
<small>FRBC BSA/AML Examination Manual</small>	<small>121</small>	<small>6/25/2005</small>	<small>FRBC BSA/AML Examination Manual</small>	<small>122</small>	<small>6/25/2005</small>

10

Incentives to Induce Authorization

11

Incentives for Purported Authorization



12

Prime Time Checking																																																														
Account Number: [REDACTED] Statement Date: October 31, 2007 Page: 1 of 3																																																														
<p>TO OUR VALUED CUSTOMERS:</p> <p>HASSIE WILHELM ISABEL WILHELM 1000 WILHELMWOOD ROAD #500 WILMINGTON, DE 19806</p> <p>us at Info@BeneficialSavingsBank.com • For 24-hour account information call DirectLink at 215.864.1798 or 888.794.8510 • For other information visit us at www.BeneficialSavings.com</p>																																																														
Account Summary																																																														
<table border="1"> <tr> <td>Previous Statement Balance As Of 07/29/2007</td> <td>1,344.88</td> </tr> <tr> <td>Total Debits/Credit</td> <td>2,223.85</td> </tr> <tr> <td>Total Credits</td> <td>2,223.85</td> </tr> <tr> <td>Ending Balance</td> <td>1,344.88</td> </tr> </table>							Previous Statement Balance As Of 07/29/2007	1,344.88	Total Debits/Credit	2,223.85	Total Credits	2,223.85	Ending Balance	1,344.88																																																
Previous Statement Balance As Of 07/29/2007	1,344.88																																																													
Total Debits/Credit	2,223.85																																																													
Total Credits	2,223.85																																																													
Ending Balance	1,344.88																																																													
Annual Percentage Yield Earned: 0.50%																																																														
Check Summary																																																														
<table border="1"> <thead> <tr> <th>Date</th> <th>Ck# No.</th> <th>Amount</th> <th>Date</th> <th>chk# No.</th> <th>Amount</th> <th>Check Bookend</th> </tr> </thead> <tbody> <tr> <td>10/01</td> <td>1421</td> <td>41.00</td> <td>10/01</td> <td>1422</td> <td>21.00</td> <td>1</td> </tr> <tr> <td>10/01</td> <td>1422</td> <td>31.00</td> <td>10/01</td> <td>1423</td> <td>21.00</td> <td>1</td> </tr> <tr> <td>10/02</td> <td>1423</td> <td>31.00</td> <td>10/02</td> <td>1424</td> <td>21.00</td> <td>1</td> </tr> <tr> <td>10/02</td> <td>1424</td> <td>31.00</td> <td>10/02</td> <td>1425</td> <td>21.00</td> <td>1</td> </tr> <tr> <td>10/03</td> <td>1425</td> <td>31.00</td> <td>10/03</td> <td>1426</td> <td>21.00</td> <td>1</td> </tr> <tr> <td>10/03</td> <td>1426</td> <td>31.00</td> <td>10/03</td> <td>1427</td> <td>21.00</td> <td>1</td> </tr> <tr> <td>10/05</td> <td>1427</td> <td>31.00</td> <td>10/05</td> <td>1428</td> <td>21.00</td> <td>1</td> </tr> </tbody> </table>							Date	Ck# No.	Amount	Date	chk# No.	Amount	Check Bookend	10/01	1421	41.00	10/01	1422	21.00	1	10/01	1422	31.00	10/01	1423	21.00	1	10/02	1423	31.00	10/02	1424	21.00	1	10/02	1424	31.00	10/02	1425	21.00	1	10/03	1425	31.00	10/03	1426	21.00	1	10/03	1426	31.00	10/03	1427	21.00	1	10/05	1427	31.00	10/05	1428	21.00	1
Date	Ck# No.	Amount	Date	chk# No.	Amount	Check Bookend																																																								
10/01	1421	41.00	10/01	1422	21.00	1																																																								
10/01	1422	31.00	10/01	1423	21.00	1																																																								
10/02	1423	31.00	10/02	1424	21.00	1																																																								
10/02	1424	31.00	10/02	1425	21.00	1																																																								
10/03	1425	31.00	10/03	1426	21.00	1																																																								
10/03	1426	31.00	10/03	1427	21.00	1																																																								
10/05	1427	31.00	10/05	1428	21.00	1																																																								
*Deposits Open in Check Number Sequence																																																														
Other Transactions																																																														
<table border="1"> <thead> <tr> <th>Date</th> <th>Description</th> <th>Deposit(+)</th> <th>Withdrawal(-)</th> </tr> </thead> <tbody> <tr> <td>10/02</td> <td>Ac-Us Treasury 303 -Soc Sec</td> <td>565.00+</td> <td></td> </tr> <tr> <td>10/02</td> <td>Ac-Us Treasury 303 -Soc Sec</td> <td>1,344.88+</td> <td></td> </tr> <tr> <td>10/02</td> <td>Ac-Car -Convcheck Ck-000000000002444</td> <td></td> <td>-24.00-</td> </tr> <tr> <td>10/02</td> <td>Ac-Pptd -Convcheck Ck-000000000002446</td> <td></td> <td>-25.00-</td> </tr> <tr> <td>10/02</td> <td>Ac-Pst -Convcheck Ck-000000000002447</td> <td></td> <td>-25.00-</td> </tr> <tr> <td>10/02</td> <td>Ac-App -Convcheck Ck-000000000002448</td> <td></td> <td>-25.00-</td> </tr> <tr> <td>10/03</td> <td>Ac-Ptm -Convcheck Ck-000000000002445</td> <td></td> <td>-25.00-</td> </tr> <tr> <td>10/05</td> <td>Ac-Sdd -Convcheck Ck-000000000002450</td> <td></td> <td>-25.00-</td> </tr> <tr> <td>10/05</td> <td>Ac-Doll Main Office -Convcheck Ck-000000000002449</td> <td></td> <td>-25.00-</td> </tr> </tbody> </table>							Date	Description	Deposit(+)	Withdrawal(-)	10/02	Ac-Us Treasury 303 -Soc Sec	565.00+		10/02	Ac-Us Treasury 303 -Soc Sec	1,344.88+		10/02	Ac-Car -Convcheck Ck-000000000002444		-24.00-	10/02	Ac-Pptd -Convcheck Ck-000000000002446		-25.00-	10/02	Ac-Pst -Convcheck Ck-000000000002447		-25.00-	10/02	Ac-App -Convcheck Ck-000000000002448		-25.00-	10/03	Ac-Ptm -Convcheck Ck-000000000002445		-25.00-	10/05	Ac-Sdd -Convcheck Ck-000000000002450		-25.00-	10/05	Ac-Doll Main Office -Convcheck Ck-000000000002449		-25.00-																
Date	Description	Deposit(+)	Withdrawal(-)																																																											
10/02	Ac-Us Treasury 303 -Soc Sec	565.00+																																																												
10/02	Ac-Us Treasury 303 -Soc Sec	1,344.88+																																																												
10/02	Ac-Car -Convcheck Ck-000000000002444		-24.00-																																																											
10/02	Ac-Pptd -Convcheck Ck-000000000002446		-25.00-																																																											
10/02	Ac-Pst -Convcheck Ck-000000000002447		-25.00-																																																											
10/02	Ac-App -Convcheck Ck-000000000002448		-25.00-																																																											
10/03	Ac-Ptm -Convcheck Ck-000000000002445		-25.00-																																																											
10/05	Ac-Sdd -Convcheck Ck-000000000002450		-25.00-																																																											
10/05	Ac-Doll Main Office -Convcheck Ck-000000000002449		-25.00-																																																											
Beneficial Savings Bank • 630 Walnut Street • Philadelphia Pa 19106																																																														

13

From Target Gift Card to Automated Electronic Mortgage Payment																																																		
<p>WACHOVIA</p> <p>P.O. Box 900001 Raleigh, NC 27675-9001</p> <p>MORTGAGE STATEMENT</p> <p>ACCOUNT INFORMATION: Statement Date: 10/05/06 Loan Number: Interest Rate: 5.9900 NEXT PAYMENT DUE DATE: 11/01/06 Current Payment: \$849.28 P U O T H Cu Cu</p> <table border="1"> <thead> <tr> <th colspan="2"></th> <th>Other</th> <th>149.28</th> </tr> </thead> <tbody> <tr> <td colspan="2"></td> <td>\$9.00</td> <td></td> </tr> <tr> <td colspan="2"></td> <td>\$9.00</td> <td></td> </tr> <tr> <td colspan="2"></td> <td>\$9.00</td> <td></td> </tr> </tbody> </table> <p>Philadelphia PA 19144-3725</p> <p>Property Address: PHILADELPHIA PA 19144</p> <p>Activity Since Your Last Statement:</p> <table border="1"> <thead> <tr> <th>Date</th> <th>Description</th> <th>Principal</th> <th>Interest</th> <th>Escrow</th> <th></th> </tr> </thead> <tbody> <tr> <td>08/01</td> <td>Payment</td> <td>\$175.59</td> <td>\$764.69</td> <td></td> <td></td> </tr> <tr> <td>09/01</td> <td>Payment</td> <td>\$176.46</td> <td>\$783.82</td> <td></td> <td></td> </tr> <tr> <td>10/02</td> <td>Payment</td> <td>\$177.35</td> <td>\$782.99</td> <td></td> <td></td> </tr> </tbody> </table> <p>Account Summary:</p> <table border="1"> <thead> <tr> <th>Loan Balance* As of 10/05/06 \$849.28</th> <th>Interest Paid Year to Date \$0.00</th> <th>Escrow Balanc... As of 10/05/06 \$0.00</th> <th>Leaves Held Year to Date \$0.00</th> </tr> </thead> </table>									Other	149.28			\$9.00				\$9.00				\$9.00		Date	Description	Principal	Interest	Escrow		08/01	Payment	\$175.59	\$764.69			09/01	Payment	\$176.46	\$783.82			10/02	Payment	\$177.35	\$782.99			Loan Balance* As of 10/05/06 \$849.28	Interest Paid Year to Date \$0.00	Escrow Balanc... As of 10/05/06 \$0.00	Leaves Held Year to Date \$0.00
		Other	149.28																																															
		\$9.00																																																
		\$9.00																																																
		\$9.00																																																
Date	Description	Principal	Interest	Escrow																																														
08/01	Payment	\$175.59	\$764.69																																															
09/01	Payment	\$176.46	\$783.82																																															
10/02	Payment	\$177.35	\$782.99																																															
Loan Balance* As of 10/05/06 \$849.28	Interest Paid Year to Date \$0.00	Escrow Balanc... As of 10/05/06 \$0.00	Leaves Held Year to Date \$0.00																																															

14

Incentives to Induce Authorization



15

Payment Processing Center, LLC

- Provides “end-to-end solutions” for telemarketing merchants
- Specializes in “Bank Draft origination for telephone **transactions that may be prohibited**” by NACHA rules

16

: lmeojhjhcbcbcapbcmlebhcaaa.justin@paymentprocessingcenter.com
= 0000000353
: 0000000D8B3FD5A785EC54E87ADC17FEBD9131424232100
: To the fine people that made hellish phone abuse a little more bearable,

I am glad to have shared the daily death-threats, hate-filled rants, and ignorance with all of you. I think sometime in the next couple weeks I may almost (in some kind of sick way) miss the sound of shit-kickers screamed obscenities over the verification playback.

bacon-speckled tomato soup, dealt with a phonebook's worth of customer callbacks, and a lot of soggy bread from the sandwich club.
When you come into work on Monday don't be sad that my cute little ass isn't around, be happy... because finally one of us will get to know what daylight looks like during a weekday. Just remember my million fangs and howl at moon

I know the customer service number and I'm not afraid to call with my bank rep on the line)

17

Now, as I hang up my Steno Pad and descend back into a world of relative normality I would like to say THANK YOU to everyone.

Side note to Michael: How much exactly do I owe you for the knowledge that it takes a total of 16 combined brain cells and teeth to provide your bank account information to a stranger on the phone to order something with as stupid a name as Washballs? or; the knowledge that old people are just plain easy to trick?

stay in touch,
Justin

18

Purported Authorization Obtained By Telemarketer



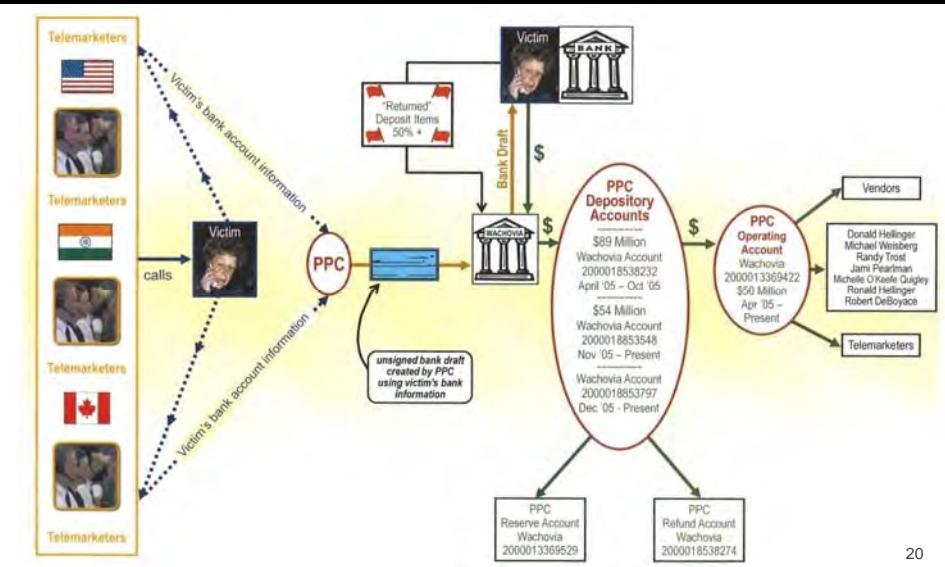
David XXX, Sr.
1933-2006

*University Football Coach
Little League Coach
Sunday School Teacher
Husband, Father,
Grandfather, Brother*



19

The Payment Process



20

A Mutually Profitable Relationship!

Dollar value of RCCs deposited by PPC with Wachovia in 12-month period: **\$162,000,000**

Income from RCC fees:

PPC – approx. \$8,000,000

Bank – approx. \$1,900,000



21

Wachovia: Victim or Participant?

- Knew or remained willfully blind to fact that PPC serviced mass market fraudsters
- Ignored glaring red flags
- Suppressed internal concerns
- Ignored express warnings from other banks
- Entered agreements with PPC to protect its own interests at the expense of the interests of other banks and their customers

22

Failure in Due Diligence PPC's Telemarketing Merchants



- Facially suspicious product offers and marketing scripts
 - Grant offers
 - Prescription discount cards
 - Travel Programs
 - Free Gift Cards
 - Free Computers
- Merchants mostly based overseas and/or using foreign banks
- Exploited names of legitimate companies, such as Wal-Mart, K-Mart, Home Depot, Carnival Cruises, AIG

23

Eyes Wide Shut



- PPC merchants were fraudsters well-known to Better Business Bureaus, state Attorneys General, and consumer protection websites
 - Star Communications
 - Advantage America
 - Suntasia
- As successive payment processors were shut down by law enforcement, Wachovia continued to process RCCs for same fraudulent merchants

24

Returns – Charge Backs

- At inception, Wachovia **anticipated returns exceeding 35 percent** (compared to approximately 1/2 of 1 percent for all checks)
- Actual returns exceeded **50 percent**
- Wachovia charged PPC substantial fee for returns
- Wachovia offered PPC volume discounts on return fees



25

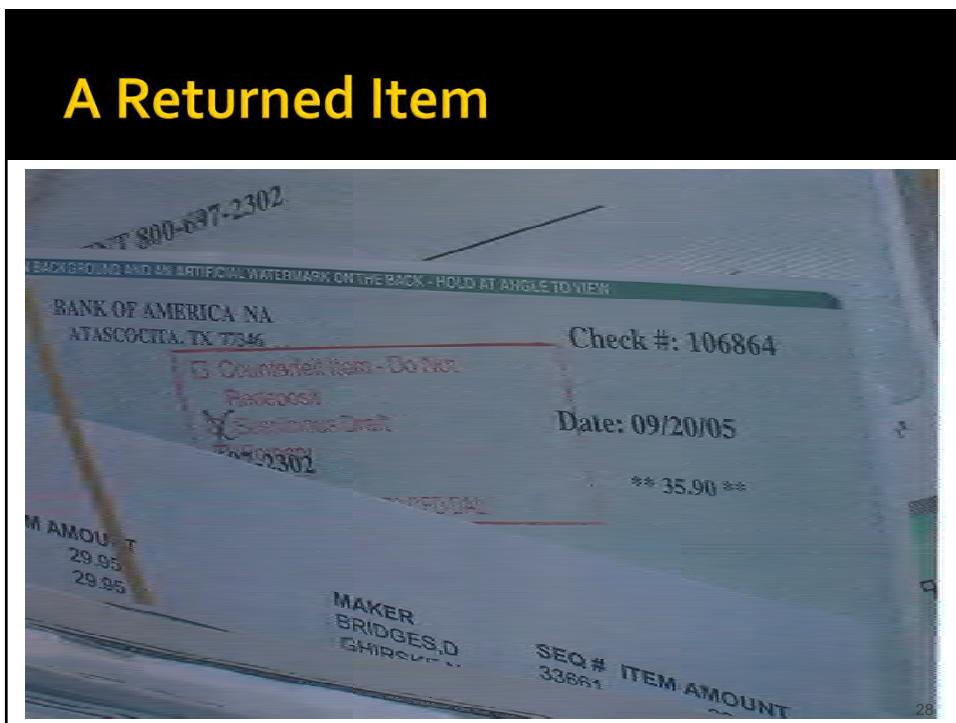
Return Reasons

- More than 50 percent of PPC's returns facially identified as:
 - UNAUTHORIZED
 - FRAUD
 - REFER TO MAKER
- Every month Wachovia received and hand-processed thousands of **sworn affidavits from consumers alleging that PPC debit transactions were not authorized**

26

Bank of America, N.A.	
AFFIDAVIT OF UNAUTHORIZED CONSUMER DRAFT	
(Type or Print Name)	
Bank:	Bank of America, N.A.
Banking Center:	229 Commerce St
RC:	3360
Telephone #:	207-754-6745
Use this form for drafts with the following item codes only: 184 POD Check 181 Credit	
Customer's Name:	Account Number:
Street:	Line 1
City:	MA 01604
	P.O. Box
	Daytime Telephone
	Home Telephone
I declare, swearing under oath, that a draft charged to my account and appearing on my account statement is UNAUTHORIZED.	
Check appropriate Section I OR Section II: I. Draft Never Authorized: <input checked="" type="checkbox"/> I have never authorized the company named above to debit my account.	
<input type="checkbox"/> I authorized the company named above to debit my account, but I revoked ** the authorization on _____ <small>** Customer must provide Bank with a copy of the written revocation</small>	
<small>I further declare that the above transaction was not initiated by me or by any person acting on my behalf. In signing this form, I understand that the Bank will remit any credit(s) to my account if it receives proof from the payee of the draft that I, in fact, authorized this draft.</small>	
<p style="text-align: center;"><i>5-12-05 [Signature]</i></p>	
<small>FOR USE ON PERSONAL ACCOUNTS ONLY</small>	
<small>Instructions:</small>	
1. File in Adjustment Department 207-754-6310	OR Send a copy of the returned item (if available) and the signed affidavit through Interoffice mail to: Adjustment Department ME001-31
2. Place a stop payment for the amount of the draft on this customer's account to prevent any future drafts from processing to this account. Have customer sign Stop Payment Order and return form to us.	
3. Advise customer that provisional credit will NOT be granted on this transaction. Customer account will only be credited upon bank receiving credit back from draft enforcer.	
<small>184 of Unauthorized Consumer Draft Rev 05/04</small>	

27



28

A Box of Returned Items



A Room of Boxes of Returned Items



30

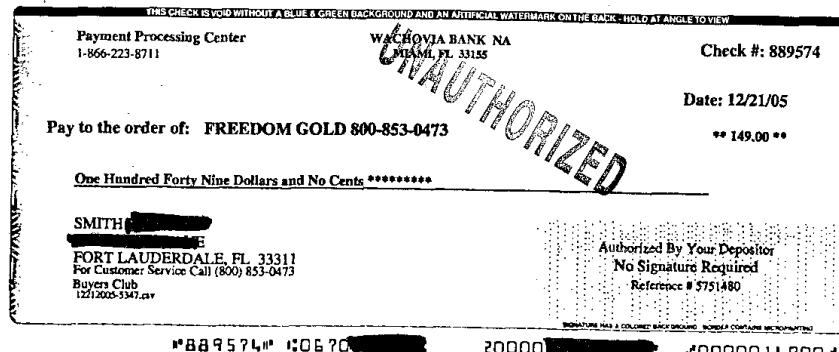
Outlier Business Practices



- PPC regularly transferred large amounts of money to overseas accounts.
- Wachovia allowed PPC to deposit RCCs payable to third-party merchants into its own accounts – without agency agreements.
- The Wachovia/PPC business model was based on large volumes of returns – an ordinarily suspect and undesired result.
- Wachovia's own customers often treated differently than other banks' customers.

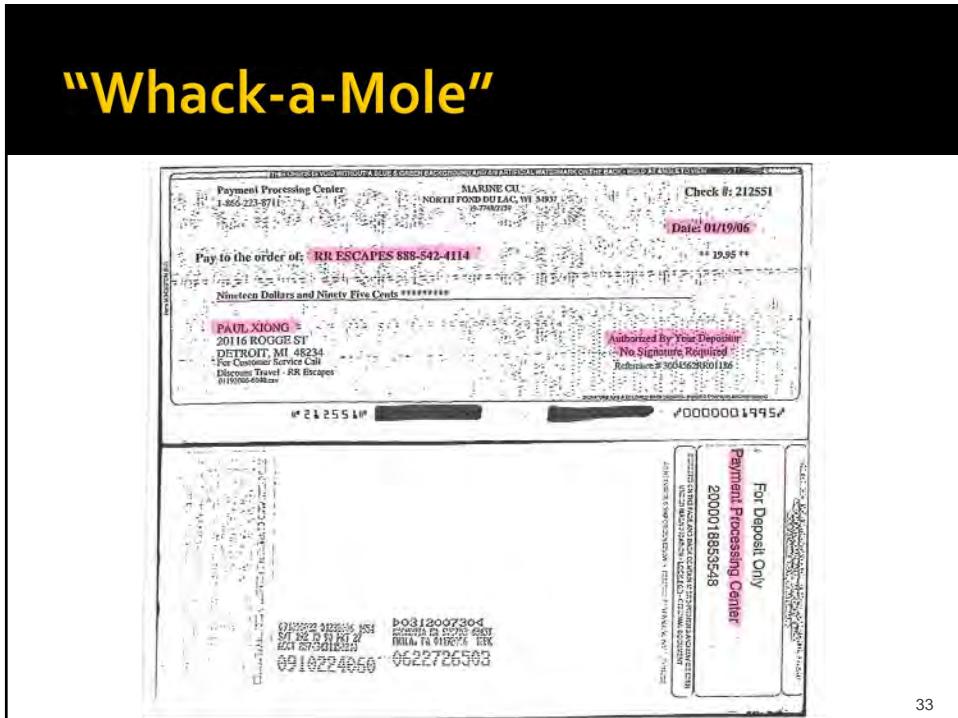
31

"On the House" Returns



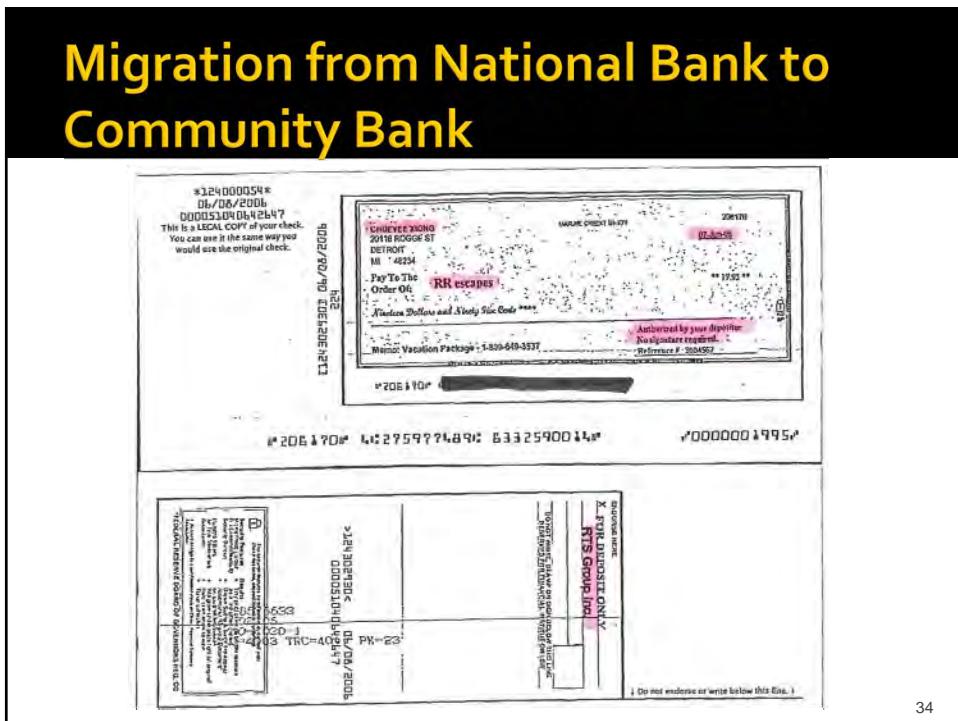
32

“Whack-a-Mole”



33

Migration from National Bank to Community Bank



34

Wachovia Ignored Internal Concerns

Return “volumes are tremendous” and “payment of these items is not our normal process”

Returns Operations Supervisor to VP of Loss Management

“Nothing [PPC] could ever do would make me comfortable . . .”

Bank Loss Management Official after learning about Bank relationship with PPC

After Loss Management official recommended closing PPC accounts, wrote “business line has assumed risk for the customer and decided to keep their accounts open”

Communication between Bank Loss Management Officials

35

Wachovia Ignored Internal Concerns

“Please consider the regulatory and reputational risks involved here. **We have now been put on notice that accounts at [Bank] are being used . . . to further these schemes.**

“If PPC has in place ‘a standing agreement with [Bank] to pay all claims without dispute,’ then they know they have rogue telemarketers in their customer base.”

Internal E-mail from Bank’s In-house Counsel after receiving fraud warning from another bank

36

DOUBLE YIKES!!!!

 08/23/2005 06:35 PM
To :
cc :
Subject: Guardian Marketing # 2000027007068

Tom,
Bob, Tim & I need to huddle with you on this account relationship. It is a Business Banking account, it has been actively making deposits since 6/23/05 and there is a current balance of \$743,000+ in the account.
The account came to us from B of A (so we are advised by : [redacted] in Bus. Bnkg.) and she is

ALL their deposits are THIRD PARTY DRAFTS!!! DOUBLE YIKES!!!!

YIKES!!!! Moreover, the drafts that are being deposited and are charging back, are not \$99.99; these items are all over the place in terms of their amount. Moreover, there is another account, Suntasia, #2000027027721. Same address, same principals. \$ from the Guardian acct is transferred to Suntasia and then the \$ is wired out to Bank of America (funny, I thought I said they were leaving B of A at the beginning of this note didn't I?). And, there is more, but nothing more that I want to put into a note. Bob...
And, there is more, but nothing more that I want to put into a note. Bob and I really need to talk to you on tomorrow.

Thanks,

37

Wachovia Ignored Explicit Fraud Warnings From Other Banks

"The purpose of this message is to **put your bank on notice of this situation and to ask for your assistance in trying to shut down this scam . . .** instigate an investigation into whether [PPC is] conducting legitimate business and whether [Bank is] getting **a high volume of return items on those accounts (that should place your bank on notice of potential fraud).**"

E-Mail from Citizens Bank

38

Bank's "Oral Agreement" With PPC To Pay All Returns

- Intended to protect Bank's reputation rather than consumers

"[I]f we can find a way to pay the returns . . . without sending them back to other banks, I think that will go a long way to preserve our reputation. **The sooner the complaint gets paid the quicker it goes away.**"

Internal Bank e-mail

- Demonstrates that UCC warranty rule is not an effective anti-fraud tool

39

Money Motivates



"[P]lease mark your calendar – we will take them somewhere nice for lunch. We are making a ton of money from them."

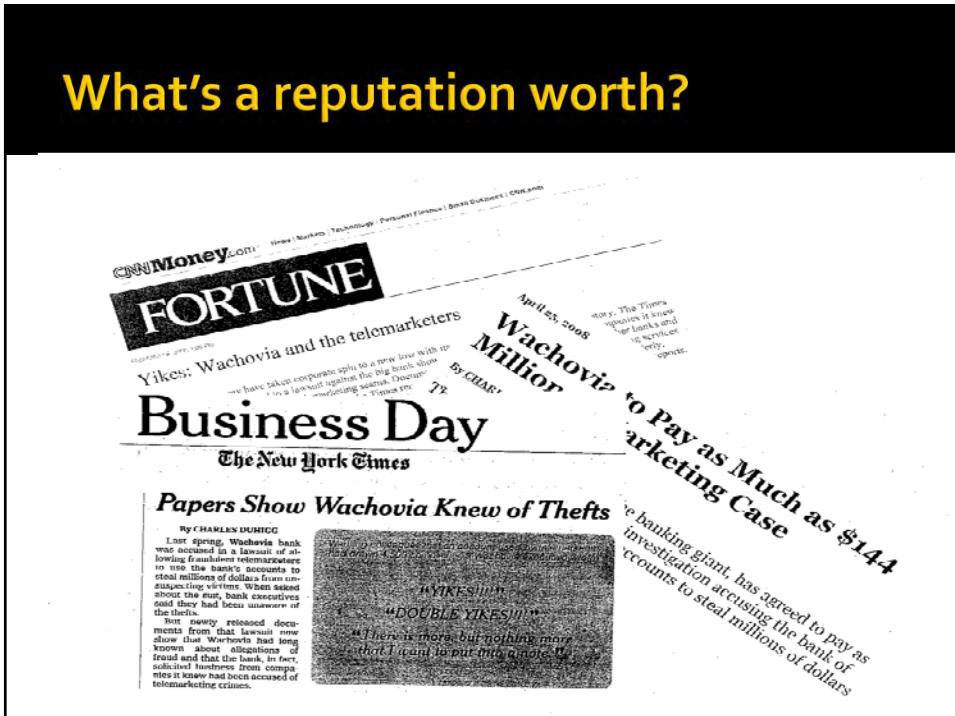
Bank Relationship Manager to Senior Business Development Officer

"[T]his is our most profitable account. \$1mm per year in profit. They have asked for Eagle tickets. What can we do?? They deserve them with all we make from them."

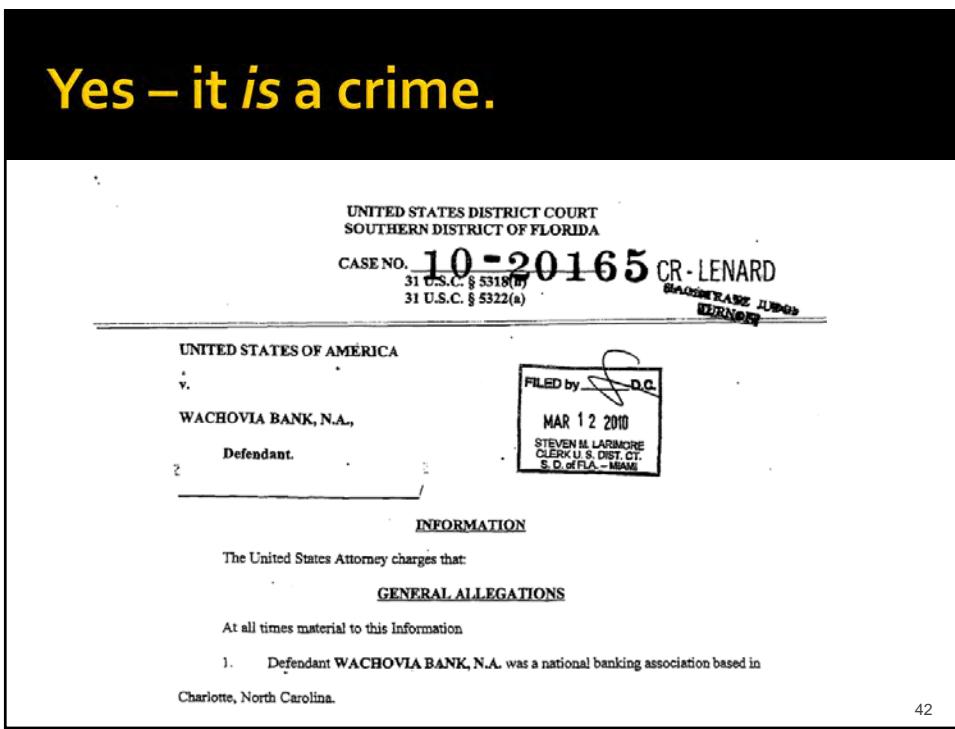
Bank Relationship Manager to Senior Business Development Officer

40

What's a reputation worth?



Yes – it *is* a crime.



It's not over until it's over.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA : CRIMINAL NO. 11-
: DATE FILED: February 10, 2011
v.
: VIOLATIONS:
DONALD HELLINGER : 18 U.S.C. § 371 (conspiracy – 1 count)
RONALD HELLINGER : 18 U.S.C. § 1960 (operating an illegal money
MICHAEL WEISBERG : transmission business – 1 count)
RANDY TROST : 18 U.S.C. § 1955 (operating an illegal gambling
JAMI PEARLMAN : business – 1 count)
MICHELE QUIGLEY : 18 U.S.C. § 1084 (transmission of wagers and
: wagering information – 8 counts)
: 18 U.S.C. § 1956(a)(2)(A) (international money
laundering – 3 counts)
: Notice of forfeiture

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES THAT:

At all times relevant to this indictment:

BACKGROUND

I. Defendants DONALD HELLINGER, RONALD HELLINGER,
MICHAEL WEISBERG, RANDY TROST, JAMI PEARLMAN, and MICHELE QUIGLEY

43

Financial accountability -- thanks to federal agents,
prosecutors, and bank regulators, class action attorneys,
local and state law enforcement, *The New York Times*, and
many determined victims of consumer fraud !



44

A simple proposition.

Mass-market scammers need access to payment systems (RCC's, ACH, CC) to take consumers' money. Without bank access there are no unauthorized withdrawals.

Banks are stationary (no "whack-a-mole"), regulated, and are concerned about reputational risk.

Banks already are required to have systems in place to prevent criminals from accessing the banking system.

Cutting off the scammers' access to the payment systems is relatively efficient and fast, and protects consumers prospectively as we investigate.

45

Important steps forward . . .

- Guidance to banks from FDIC, OCC and FinCEN
- United States v. First Bank of Delaware
- Financial Fraud Enforcement Task Force/Consumer Protection Branch efforts to choke-off fraudsters' access to payment systems (DOJ, FTC, FDIC-OIG, USPIS, FBI, and others)
- May 21, 2013: FTC Notice of Proposed Rulemaking would ban the use of RCCs in connection with telemarketing

46

Operation Choke Point So far . . .

- More than 50 subpoenas issued to banks and TPPPs.
- Several active criminal and civil investigations.
- Banks are self-disclosing problematic TPPP relationships.
- Banks are terminating TPPP relationships and scrutinizing scammer relationships.
- Internet Payday lending – collateral benefits.
- Investigative support from USPIS, FBI, SIGTARP, USSS

47

Regulatory Loophole

- Treasury Department regulation amended in 2011 arguably excludes third-party payment processors from the definition of “money transmitter” and thus is not a Money Services Business (“MSB”).
- **A payment processor that originates tens of millions of dollars of debit transactions against consumers’ bank accounts on behalf of Internet and telemarketing merchants may not be an MSB and may not be required to register with FinCEN or comply with the BSA.**

48

Thanks for your time and interest!

Questions?

Joel M. Sweet
202-532-4663
joel.sweet@usdoj.gov