Third-Party Payment
Processing and Financial Crimes

March 14, 2012

Michael 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

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

BANKNORTH MASSACHUSETTS
BREWSTER, MA 02631
53-TD542113

Check #: 229554

Date: 05/05/05

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

** 149.90 **

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

Wilson

Worcester, MA 01604
For Customer Service Call (800) 357-8873
05052005-225.cv

Authorized By Your Depositor
No Signature Required
Reference # 11007157

Signature has a colored background - border contains microprinting
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
Due Diligence & Underwriting

- Policies and procedures
- Assessment of processors (including review of merchant clients)
- Ongoing Monitoring for:
  - Consumer complaints & audits
  - Financial institution complaints
  - High rates of returns or charge backs
  - Suspicious activity/previous record of misconduct
  - Conflicts of interest
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
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.
TPPP Resources

- Supervisory Insights – Summer 2011
- 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
- Interagency TPPP Subgroup of the Bank Fraud Working Group
Account Takeover Activity

- Sophisticated methods (malicious software, spyware, etc.) to obtain access to accounts

- Financial institutions identify inconsistencies with a customer’s normal account activity that indicates illicit intrusions into a customer’s account (unusual ATM activity, clustered ACH transactions in different geographic areas, sudden wire transfers, or changes to account profiles)

- Account takeover activity differs from other forms of computer intrusion, as the customer, rather than the financial institution maintaining the account, is the primary target
Account Takeover Activity (Cont.)

- **Computer intrusions (accessing a computer system of a financial institution):**
  - Remove, steal, procure or otherwise affect funds of the financial institution or the institution’s customers;
  - Remove, steal, procure or otherwise affect critical information of the financial institution including customer account information; or
  - Damage, disable, disrupt, impair or otherwise affect critical systems of the financial institution.

- **At least one target of account takeovers is a customer account at the financial institution**

- **The ultimate goal is to remove, steal, procure or otherwise affect funds of the targeted customer**
Long Term Cyber-Related
Estimated Fraud Loss Trends are Down

Year-to-Year Fraud Trends

$ Loss Millions

2006 2007 2008 2009 2010 2011

Computer Intrusion
Wire Transfer (and ACH)
Payment Card
Check-Related
ID Theft
SAR Reporting of Account Takeovers

- Financial institutions should use the term “account takeover fraud” in the narrative section.

- Provide a detailed description of the activity.

- Enhance the usefulness of SAR filings:
  - If the account takeover involves computer intrusion, check the box for “computer intrusion.”
  - Financial institutions can check the “other” box and note “account takeover fraud” in the space provided.
If other delivery channels are involved (i.e., telephone banking, social engineering) check the “other” box, note “account takeover fraud,” and describe the additional information in the space provided.

If the account takeover involves a wire transfer, check the “other” box and note “account takeover fraud” AND check the “wire transfer fraud” box.

If the account takeover involves an ACH transfer, check the “other” box and note “account takeover fraud – ACH”.

Because account takeovers often involve access to PINs, account numbers, and other PII, financial institutions may ALSO need to check the box for “identity theft.”

Additional boxes should be checked if appropriate (e.g. “terrorist financing”)
Questions?

Thank you!