

May 11, 2010



Business Banking Authentication

Next Steps

George Tubin
Senior Research Director

Agenda

Our overarching point of view

Effective technology point solutions

A fraud prevention framework

Two Ominous Threats (among others)

Man in the Browser (MITB)

- Inserts forms to collect data
- Usurps authenticated user session
- Executes fraudulent transactions

Social Engineering

- Basic credentials captured via malware
- Fraudster prepares session
- Fraudster contacts user to obtain additional authentication information

The Bottom Line

**SMBs simply cannot protect themselves
from these threats!**



Banks Must Take Responsibility

and/or

Congress Must Act

Emerging Fraud Prevention Technologies

- Mobile transaction authentication
- Secure browser plug-in
- Behavioral monitoring
- Knowledge-based authentication
- Mobile geolocation
- Reverse positive pay
- ACH debit blocks
- Biometrics
- Enterprise fraud prevention



Dedicated PC for Online Banking?



What about integration with:

- POS system?
- Accounting software?
- Invoice management?
- Payroll system?

What about:

- Social engineering?
- Cost?

Out of Band Transaction Authentication

Key attributes:

- Out of band
- Mobile application or SMS
- Transaction information included
- Risk-based
- Customizable
- Alerts on other predefined transaction types



Source: Entrust

Secure Browser Plug-in

Key attributes:

- Software download
- Website authentication
- Keystroke encryption
- Browser lockdown
- Identify and remove threats



In-Session Behavior Monitoring

Key attributes:

- Pre and post authentication
- Activities and transactions
- Page navigation and transaction speed
- Compare to “normal” for user and others



Layered Security Is The Key to Fraud Prevention

Proactive Monitoring

Brand monitoring, honey pots, black market site monitoring, info sharing, etc.

Authentication

Secure cookie, IP intelligence, HTTP header, OTP, KBA, OOB, secure browser, etc.

Transaction Monitoring/Behavioral Profiling

Fraud pattern matching, velocity calculations, behavioral monitoring, etc.

Batch Fraud Monitoring

Link analysis, pattern recognition, preemptive forensics, etc.

Customer Involvement

Education, Web tools, preset limits, interactive alerts, outbound calls, etc.

Questions

gtubin@towergroup.com