The Rise in Online Banking Fraud

Internet usage and the online banking sector are experiencing spectacular growth. Worldwide, there are over a billion Internet users at present. In North America, the percentage of the population with Internet access is at 68%\(^1\). Online banking has been the fastest growing Internet activity in the U.S. over the last five years, with 53 million users, or 44 percent of the U.S. population\(^2\). This growth in popularity has not gone unnoticed by the criminal element.

Online fraud has become major source of revenue for criminals all over the globe. This has made detecting and preventing these activities a top priority for every major bank. Reuters reports that according to a US Treasury advisor Valerie McNiven the broad category of Global cyber-crime turned over more money than drug trafficking last year\(^3\). Most disturbing is the recent increase in the number of attacks and the evolution of their techniques. Recently, the Anti-Phishing Working Group released a report that noted November 2005 as the all time high for reported Phishing attacks\(^4\):

- In November over 2000 companies, ISPs, and banks reported 16,882 unique phishing attacks
- Representing a 21% increase over October 2005
- Report also noted an increase in the number of URLs hosting malicious code that steals passwords

The corresponding web sites belong to online financial services and online commerce sites, ranging from small branch offices to international groups. This shows that these malware are no longer a small local phenomenon.”

Key Types of Online Fraud

There are two classes of fraud that commonly affect online operations:

1) **User Identity Theft**: the user information required to obtain access to the online systems is stolen through means that include:
   - Phishing attacks which trick the user into providing access information.
   - Key-loggers and "spyware" which transparently capture access information.

2) **User Session Hijacking** - an attack in which a user’s activities are monitored or falsified using malicious software (“malware”). Session hijacking malware can operate on a user’s local computer, or remotely as part of a “man-in-the-middle” attack.
   - Local malware session hijacking uses techniques such as host file redirects.
   - Remote malware session hijacking attacks use techniques such as DNS hijacking and Content Injection.

Strong authentication at the “Front Door”, while valuable, provides only partial protection against User Identity Theft. However, this approach provides no protection against Session Hijacking.

This paper describes how the basic “Front Door” Two-Factor Authentication solutions can be coupled with Behavioral Analytics (“what you do” protection) to provide a solution that affords good protection without compromising customer experience.

The Spirit of the FFIEC Guidelines

To help combat fraud the FFIEC (Federal Financial Institutions Examination Council) issued guidance on October 12th, 2005 related to stronger authentication for Internet banking services. Financial Institutions are expected to achieve compliance by year-end 2006.

**Highlights of the FFIEC Guidance:**
- Financial institutions offering Internet-based products and services should use effective methods to authenticate the identity of customers using those products and services.
Single-factor authentication methodologies may not provide sufficient protection for Internet-based financial services. The FFIEC agencies consider single-factor authentication, when used as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.

“The common approach of front-door authentication is an important hurdle to place in the way of fraudsters, but identity thieves often have the information to pass through that gateway. With the addition of real-time fraud detection, single users and group-level activity can be intelligently monitored for patterns that are an instant tip-off to fraud,” notes George Tubin, Principal at Tower Group, a leading analyst firm. “Even more compelling is that this can be done without disturbing the customer experience. Institutions that are not just watching the door, but also keeping an eye on the user activity on their sites, are meeting the true spirit of the FFIEC guideline.”

## Mutual Multi-Factor Authentication

A big reason for the success of the Internet is that you can access the applications from anywhere. This coupled with the simplicity of the HTTP protocol makes it easy to steal and spoof identity.

### Basic Front Door Authentication

Consists of three parts:

1. **Single Factor Authentication** – Basic username/password authentication (What you know)
2. **Multi Factor Authentication** – Could be software-based where a device ID is installed using a cookie or an plug-in, hardware-based approaches with smartcards and USB tokens (What you Have) or out-of-band approaches of one-time pass-code via SMS or Email channel etc. These methods have varying levels of security and impose different levels of inconvenience to the end user.
3. **Mutual Authentication** - gives the user a simple way to verify that they are really connected to the intended online institution before providing sensitive information.

What is described above provides some protection against basic phishing attacks, but they don’t provide sufficient protection against the more sophisticated “malware” attacks. To protect against these threats, a more comprehensive and sophisticated approach is required supported by the Behavioral “What you do” information.

### Zero Touch Multi Factor Authentication

Zero Touch Multi-Factor Authentication goes far beyond basic two-factor authentication, and allows online businesses to protect their customers with behavioral authentication without impacting user experience. The fundamental approach is to supplement standard authentication with “intent-based” detection, which keeps a behavioral profile of each customer based on his or her activity, examines deviations from the normal and detects fraudulent intent - providing transparent, adaptive, and continuous protection.

Some of the factors considered by the Business Signatures solution are:

- **Credential Risk**: Does the user have the correct password and other personal data expected?
- **Transaction Risk**: Is the user trying to make a payment over a threshold amount or change passwords or other personal security information.
- **Location Risk**: Is the user coming from an approved or previously authenticated Internet location with an expected Browser Profile and Computer Profile?
- **Behavioral Risk**: Is the user coming at an unusual time of day, performing a transaction involving an unusual payee, or unusual amount given that users past behavior? Behavioral Analytics as applied to Mutual Multi-Factor Authentication is further described below.

In order to reduce the inconvenience to the end user, the second factor questions are often not asked unless a high-value or high risk transaction is to be performed. In other words, a bank may allow users to logon and check their balances with only a single-factor authentication, but a second factor is required to perform a funds transfer or change the account password.

The Business Signatures solution to the authentication problem uses a flexible scoring technique where each factor in the process is assigned a confidence score. A running score is kept during the stages of the
authentication process. Any behavioral deviations are considered with other factors such as logon location. This score is used to determine whether to admit the user after a given step or ask for more validation information. The solution also addresses the mutual authentication needs through use of a dynamic watermark displayed by the bank consisting of a secret word, name, date & time. This provides the user the assurance they are interacting with the official and safe banking site before they enter their password.

**Regular 2 Factor Authentication combats phishing identity theft**

![Regular 2 Factor Authentication Diagram]

**Only Behavioral 2 Factor Authentication combats "man in the middle" attacks**

![Only Behavioral 2 Factor Authentication Diagram]

**The e-Fraud Library™**

Business Signatures’ Real Time e-Fraud Detection (RTFD) product continuously processes all online customer interactions, at the individual level, in real time. With this incisive visibility into all aspects of your customers’ online interactions the system can detect suspicious behavior and interdict with unprecedented precision before fraudulent transactions occur. That means uninterrupted, safe, and secure online transactions for your customers without having to change their behavior.

Business Signatures offers a continuously refreshed library of e-Fraud Rules that provide out-of-the-box protection against fraudulent activity that only Business Signatures can detect. This library delivers state-of-the-art patterns of fraudulent behavior encoded into Fraud Rules according to vertical industry characteristics. You can adjust the parameters of these signatures to define the level of risk your fraud team determines appropriate for your enterprise. You also determine the risk score for each Fraud Rule (low, medium, high) and set alerts and interventions accordingly. Moreover, you can define custom Fraud Rules to maximize your competitive advantage in protecting your enterprise.

When the Business Signatures Mutual Multi-Factor Authentication Solution is combined with the Business Signatures e-Fraud Prevention Solution, it can interact with the e-Fraud Library to consider patterns of activity within the user’s current session:

- Is this logon location, payee or wire transfer destination on a "black list"?
- Has the user changed their security information AND is now trying to make an unusually large payment
- Is this session being initiated from a referring URL from an "email" location?

Patterns of activity from other sessions and other users can also be considered during authentication:

- Have there been multiple failed login attempts from this same location in the last 24 hours?
- Have there been multiple successful logins from this same location in the last 24 hours?
- Have other users recently added the same payee and made large payments in the same session?
- Has this same user logging on from another geographically distant locations within a given time period?
Evaluating e-Fraud Prevention Solutions

With the number and sophistication of e-fraud attacks growing, it is critical to protect your online sites with more than just simple single factor authentication. There are several things to consider when evaluating your strategy.

**Broad Protection:**
- Fraud Risk Reduction: Does the solution significantly reduce the likelihood of online fraud in your operations? How will this translate to a reduction in lost revenue?
- Fraud Coverage: How well does the solution protect against each of the common types of online fraud attacks?

**Customer Experience Impact:**
- Impact Minimized: One way to eliminate online fraud would be to entirely block access. A real solution needs to encourage use of the online enterprise by balancing frictionless access with the risks associated with specific user transactions.
- User Perception: If your online operation is perceived as having weak security, it may result in lost customers and revenue. Meeting the perceived standard is a minimum. In addition, a solution that allows users to tune their own risk/convenience security interaction may increase user satisfaction and attract customers.

**Cost of Ownership:**
- Deployment: What is the cost of the software, infrastructure and integration efforts? Does the solution fit seamlessly into your operation?
- Operations: What is the effort required to monitor and maintain the solution? How many interactions result in calls to the help desk? Can the solution easily adapt to changes in the nature of fraud and the evolution of your online operations?
- Availability: Is the solution robust and scalable? The solution should not decrease availability and result in lost revenue.
- Flexibility: Is the solution adaptable to account for future types of fraud regulations?

**The Business Signatures e-Fraud Prevention Solution:**
- More effectively addresses both types of online fraud to help you reduce your fraud exposure.
- Minimizes impact on user experience and provides flexibility for both the site and end user to tailor authentication interaction.
- Minimizes Total Cost of Ownership with minimal infrastructure requirements, flexible and painless integration and low operational costs. Ensures scalability and high availability.
- Allows increasing levels of authentication appropriate to the risk of the activity taking place.

**Summary**

The use of single-factor authentication, such as user name and password, has been inadequate for guarding against account fraud and identity theft, in sensitive online services. The introduction of additional authentication provides an added level of security.

The Business Signatures e-Fraud Prevention Solution provides an effective online fraud solution which provides protection against a wider variety of security threats without increasing the burden on the end user. This enables institutions to implement much more effective security measures, reducing their financial risk of online fraud without adding significant maintenance cost for the online application.

3. US Treasury computer crime advisor Valerie McNiven in an interview with Reuters while speaking in Riyadh at a conference on information security in the banking sector. Nov. 29th, 2005
4. InformationWeek, Jan. 20th, 2006