



## **YOUnite<sup>®</sup> Use Cases: Credit Card Processing Industry – Visa, MasterCard, American Express, Discover, Diner’s Club, et al**

### **Use Cases**

---

#### **Abstract**

This paper provides an overview of the YOUnite market opportunity for the Credit Card Industry. For the purposes of this paper, we will assume Visa has chosen to integrate YOUnite services into their platform and examine potential revenue strategies and opportunities for Visa.

*The information contained in this document represents the current view of YOUNite Inc., on the issues discussed as of the date of publication. Because YOUNite must respond to changing market conditions, it should not be interpreted to be a commitment on the part of YOUNite Inc., and YOUNite Inc. cannot guarantee the accuracy of any information presented after the date of publication.*

*This white paper is for informational purposes only. YOUNite Inc. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of YOUNite Inc.*

*YOUNite may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from YOUNite, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*© YOUNite Inc... All rights reserved. YOUNite<sup>®</sup>, YOUNite Enterprise<sup>®</sup>, YOUNite Mobile<sup>®</sup>, YOUNite Community<sup>®</sup> and YOUNite Webtop<sup>®</sup> are registered trademarks of YOUNite Inc. in the United States and/or other countries.*

*Other product and company names mentioned herein may be the trademarks of their respective owners.*

*YOUNite Inc. • 650 Castro Street – #120-377 • Mountain View, CA 94043 • USA • 866,794.4968*

*06/2008*

---

## Contents

<b>Introduction</b> .....	<b>1</b>
<b>Use Case 1</b> .....	<b>2</b>
Relevant 1-to-1 Targeted Marketing	2
<b>Use Case 2</b> .....	<b>4</b>
Identity/Preference Based Fraud Detection	4
<b>Use Case 3</b> .....	<b>7</b>
Online Pre-authorization Validation via SMS or E-mail Services	7
<b>Use Case 4</b> .....	<b>9</b>
Federated Identity Management for Financial Transactions	9
<b>Summary</b> .....	<b>11</b>



---

## Introduction

YOUnite is a flexible platform that allows users to create secure, personal-attribute and personal-preference data exchanges to enable an entity (business or individual) to securely distribute these details on a user-controlled and customized basis without having to store that information on a centralized server. Our technology is platform independent, scalable, and cost-effective.

This collection of use cases explains the importance of distributed infrastructure technology to the Credit Card Processing industry and those companies that seek to grow revenue by becoming a center of a revolutionary global personal information interchange through a solution enabling distributed sharing of personal information and attributes. This collection of use cases highlights the unique patent-pending capabilities and potential revenue strategies when integrating YOUnite into existing systems.

These cases also highlight the incredible opportunity available to a company seeking to be the leader of a revolutionary global information interchange platform that provides distributed sharing of user-managed personal identity information and preferences.

The YOUnite Enterprise® Interchange is a patent-pending technology that is capable of sustainable revenue generation provided by endless partnerships that benefit from access to the most valuable and accurate customer information ever—user-managed personal identity information and preferences. YOUnite connects the customer with the marketplace like no one has done before.

---

## Use Case 1

### Relevant 1-to-1 Targeted Marketing

#### **Summary:**

This case discusses the opportunity of targeted marketing offers to customers based on their elected sharing of personal identity information and preferences to specific retailers and service providers. This data is validated both by customer purchase history as well as customer approval authorization.

This use case examines the potential of creating relevant 1-to-1 targeted marketing offers to existing consumers through YOUNite's identity and preference technologies deployed into Visa's global transaction platform.

With a YOUNite enabled service, a credit card user now has the ability to propagate his or her relevant personal identity information and preferences to those retailers and/or service providers with whom the credit card user has an affinity relationship – for example clothing sizes and favorite colors or materials to The Gap, Nordstrom and Macy's, a broad range of likes and dislikes to Amazon.com, or their favorite beverage to Starbucks. Because Visa has developed a trusted relationship with each individual credit card user as well as a vast comprehensive network of retailers and service providers, Visa can now provide a new and exciting YOUNite enabled service to the card user as well as highly-focused and valuable 1-to-1 targeted marketing data to its vast network of merchants.

By implementing the YOUNite Enterprise®, Visa can now create a new revenue stream by selling this laser-focused marketing data to millions of retailers and services providers while at the same time providing a free valuable and personalized new service to its credit card users.

#### **Description:**

YOUNite Enterprise® is a set of server infrastructure facilities and services that allow individuals to connect and share information based on the permission settings set by them.

By integrating YOUNite Enterprise® into Visa's global network, Visa can facilitate the exchange of information between credit card consumers and retailers or other service providers. This identity information can consist of any combination of personal identity information (e.g. shirt size, eye color, skin color, hair color) or preferences (e.g. favorite colors, favorite wines, window or isle seating, smoking or non-smoking hotel rooms or even book genre preferences).

Here is how the scenario works...

A credit card user provides his or her personal information and preferences into the YOUNite enabled Visa network. Visa then enables the consumer to selectively share this identity and preference data to Visa merchants. Upon approval from the card user, Visa can then offer this extremely accurate and highly-targeted marketing data to the credit card user's preferred Visa approved

---

merchants and service providers. A fee is charged by Visa to its vendors (i.e. the retailers and service providers) while the credit card user is offered this as a free personalized Visa “concierge” service.

The retailers and service providers are now able to provide compelling special offers, sale notifications and new product offerings to highly motivated existing customers, while Visa is simultaneously provides its credit card users with a loyalty enhancing free benefit -- all within the trusted and secure Visa network.

The deployment of the YOUNite Enterprise® synthesizes targeted marketing with personalized concierge services in a manner that enables Visa to enhance and create additional revenue streams by facilitating this new value-added transaction.

**Results:**

The credit card user is provided with compelling, relevant offerings and notifications that are tailored to his or her personal preferences and attributes. The retailers and service providers are targeting pre-approved existing customers via knowledge of credit history or credit limit, who have expressly requested that these types of notifications through YOUNite’s connection and selectively sharing framework. Visa provides the interchange that facilitates the transaction thereby strengthening the loyalty of existing credit card users, enhancing the opportunity to gain market share through this service, and creating a revenue stream through the service offering to the retailers and service providers.

---

## Use Case 2

### Identity/Preference Based Fraud Detection

#### Summary:

This use case discusses the opportunity of a Visa / YOUNite enabled fraud detection service based on YOUNite's shared personal identity information and preferences. Specifically, this is accomplished through a mobile phone number tied to Visa's knowledge of merchant locations. This fraud detection solution can also be extended to location-based services for in-store or retailer transactions using GPS and/or nearest cell tower or last-call-location methods of determining consumer's actual location at time of transaction.

Credit card processors have sophisticated software in place to monitor transactions for every consumer account. These protocols understand a user's past spending pattern and can flag new transactions that deviate from that pattern. Below are a few scenarios whereby using the YOUNite Enterprise® solution, Visa's fraud detection schemes are enhanced, while minimizing false fraud incidents and catching previously missed fraud attempts:

A typical example involves a couple that takes a once-in-a-lifetime vacation to Greece and their credit card transactions are denied because Visa's fraud detection systems have never seen a transaction from Greece in the past for this consumer.

When the software flags a potential fraudulent transaction, most existing systems immediately attempt to contact the credit card consumer at the number which is in their customer service record -- most typically their home phone. In this case, the user, who is in Greece, is likely unavailable or difficult to reach and would have their transaction denied, thus causing the merchant to make a call to Visa to verify the charge.

In an alternate case, a consumer has had their card compromised (i.e. card number stolen), even though they have their actual card in their possession. The consumer's card is fraudulently being used, but at reasonable merchants (i.e. gas stations, etc.) and Visa is unable to detect the fraud.

By integrating YOUNite Enterprise® into Visa's fraud systems, Visa would now have the ability to fine-tune its detection systems by having shared preferences and personal identity information readily available. Moreover, because YOUNite Enterprise® can be tied to multiple devices, the transactions and the immediate location of the credit card user can now be immediately determined and thus validate a transaction when the consumer is present at the merchant.

YOUNite Enterprise® and YOUNite Mobile® both enables Visa to take security and fraud protection to the next level by radically decreasing fraudulent charges while providing additional protection for the consumer as well as cost savings for the merchants.

---

## **Description:**

From the previous use case, it was established that the YOUNite Enterprise® and YOUNite Mobile® can enable the credit card user to share his or her personal preferences and attributes with Visa. Therefore, the credit card user can identify those stores or services that are his or her preferred choices. If the user shares the preference of shopping at Wal-Mart and not Target, any Target transactions could be immediately flagged as possible fraudulent activity and either denied or requiring further verification. If the user has identified that he or she purchases all electronic gadgets online from Amazon.com, then a series of expensive purchases from BestBuy.com would immediately be denied and an SMS could be sent to the user's YOUNite Mobile® registered phone to determine if the transactions are valid or fraud.

In addition, Visa can deploy YOUNite Mobile® to register where the user is by means of cell phone call locations and/or GPS systems. This means that if the credit card user has made a phone call at 2:15 PM from San Francisco, CA, it is highly unlikely that a credit card transaction that is attempted in a store in New York, NY at 3:20 PM can be legitimate. Alternatively, if Visa determines (via location based services) that the consumer is at Stanford Mall in Palo Alto, CA at 5:40 PM when a card purchase is taking place on that same consumer's card in Riverside, CA at 6:00 PM, it can immediately flag the transaction as fraud, deny the transaction and attempt to notify the consumer of the potential that their credit card has been compromised and/or duplicated by calling the consumer at the YOUNite shared contact number.

Finally, if Visa's systems register a charge at a Shell gas station in Houston, TX, but the YOUNite enabled Visa fraud system determines that the actual credit card customer's mobile devices are in Mountain View, CA via YOUNite Mobile® enabled phone, Visa can deny the charge and then send an SMS challenge to the consumer's mobile device to instantly determine if in fact that charge is valid or is fraudulent.

The deployment of both YOUNite Enterprise® and YOUNite Mobile® enables Visa to greatly expand its current capabilities in fraud detection. The YOUNite technology shifts the existing software systems from predicting patterns based on past activities to understanding current and future activities through the sharing of information and preferences between the system and the actual user. In addition, the technology can enable Visa, in some cases, to identify the user's physical location.

## **Results:**

According to a Javelin Strategy & Research report published in 2006, the average amount attributed annually to identity fraud in the United States is approximately \$56.6 billion. Of this amount, approximately 30% is attributable to stolen or lost wallets and credit cards. The credit card processing agencies and credit bureaus spend an enormous amount of money fighting fraud. The

---

YOUnite Enterprise® Interchange provides a powerful tool which seamlessly strengthens and enhances the existing software systems.

Moreover, YOUnite Enterprise® directly connects the consumer with Visa in order to combat the growing and expensive incidents of fraud. This simple notion of connecting the consumer with the credit card processing company significantly improves the detection protocols and thereby significantly reduces the loss of revenue due to fraudulent activities.

---

## Use Case 3

### Online Pre-authorization Validation via SMS or E-mail Services

#### **Summary:**

This use case offers an alternative approach to fraud detection based on shared personal identity information and preferences. In this case, YOUNite Enterprise® and YOUNite Mobile® offer Visa the opportunity to combat fraudulent credit card transactions by means of pre-authorization validation through SMS and/or e-mail related transports.

By deploying YOUNite Enterprise®, it is possible to maintain accurate and current personal preferences of the credit card user and/or a predetermined transaction amount above which the credit card user is contacted for pre-authorization validation. Combining YOUNite Mobile's® ability of connectivity through wireless devices provides an added layer of fraud protection to credit card users by Visa.

#### **Description:**

YOUNite Enterprise® enables the credit card user to share and maintain accurate and current personal information with Visa. This not only includes personal identity information (e.g. shirt size and favorite book genres), but also personal preferences (e.g. favorite clothing store or choice of online electronics retailer).

There is an increasing importance of communications and connectivity in our daily lives. This phenomenon has been termed “hyperconnected”. According to IDC, a global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, the average “hyperconnected” individual uses at least seven devices to access the network and nine connectivity applications. Since many of these devices are wireless enabled, it is possible to leverage YOUNite Enterprise® and YOUNite Mobile® to provide an added level of fraud protection by making these devices-points of verification or authentication.

Here is how the scenario works...

The credit card user shares and maintains his or her current preferred vendors and service providers with Visa. In addition, Visa and the consumer establish a predetermined transaction limit with the credit card user. If a transaction event occurs that is either not in accordance with the shared preferences of the user and/or the transaction request is above the predefined amount, Visa can immediately send an e-mail or SMS to the credit card user requesting that the transaction be validated through a code-based challenge or alternative response protocol.

The deployment of YOUNite Enterprise® and YOUNite Mobile® enables Visa to add an increased level of security and fraud detection. By combining the YOUNite technology with the ubiquity of wireless communication, pre-

---

authorization validation becomes an attractive mechanism to combat potential fraudulent activities in real-time.

**Results:**

Annual identity fraud due to lost or stolen wallets and credit cards amounts to approximately \$17 billion. This has generated business opportunities for service providers to offer various types of fraud protection systems. Implementing YOUNite Enterprise® for e-mail notification and YOUNite Mobile® for SMS notification as a means of pre-authorization validation not only allows Visa to reduce financial losses due to fraudulent transactions, but also presents Visa with another potential revenue stream by providing a value-added service to the credit card end-user.

---

## Use Case 4

### Federated Identity Management for Financial Transactions

#### **Summary:**

This use case addresses the problems associated with a consumer having to provision multiple sets of userid (Login) password pairs for online access to systems for the purposes of managing or completing financial transactions. In this case, YOUNite Enterprise® offers Visa the ability to store consumers' userid/password pairs within the YOUNite profile for the specific purpose of accessing Visa enabled merchants. This could be extended to non-financial transactions and non-Visa merchants, but for this use case we will focus on the former.

By deploying YOUNite Enterprise®, it becomes possible to complete user authentication operations without requiring the consumer to manually enter the userid/password pair for each Visa/YOUNite enabled online merchant. This simplifies the user experience by eliminating the need to remember numerous userid/password pairs, as well as adds another layer of security to the financial transaction process by previously validating the userid/password pair with the consumer through Visa.

#### **Description:**

YOUNite Enterprise® enables the credit card user to share and maintain accurate and current personal identity information and preferences with Visa. This personal identity information can also include online merchant userid/password access information. With YOUNite Enterprise®, consumers can share with Visa their userid/password pairs for each online merchant. Visa can store this data in a single secure place within the Visa system as a value added for fee service to their consumers (e.g. creating a Visa e-vault).

Visa enabled online merchants would be able to authenticate these consumers using the userid/password pair that was stored for that specific merchant, thus precluding the consumer from having to manually authenticate themselves every time they wish to shop. This not only eliminates the need for the consumer to remember the numerous userid/password pairs for each merchant, but it also reduces the possibility of fraudulent authentication.

If the merchant requires that the consumer change or update their userid/password pair, this new information would automatically be propagated to the Visa e-vault so that the consumer would not have to memorize a new userid/password pair.

In addition, Visa could establish an expiring token protocol with their enabled merchants based on where the consumer is accessing the merchant. For example, if a consumer is on holiday and therefore not at one of their automatically pre-authorized computers (e.g. their home or work computers) and they authenticate themselves at Visa, Visa could ask the consumer how long they plan on shopping. Visa could then establish a time-duration of the

---

authentication token so that it would automatically expire based on the consumer's response (e.g. one hour, one day, etc.). Therefore, any attempt to access the Visa/YOUnite enabled online merchants after expiration would require the consumer to re-authenticate themselves before completing a transaction or accessing the merchant. Not only would this approach to federated identity management protocol improve the effectiveness and efficiency of the financial transaction process, but it would also eliminate the possibility of fraud.

**Results:**

Leading enterprises throughout the world have deployed identity federation management systems to improve customer service, accelerate execution of financial transactions, cut costs and increase security. By integrating YOUnite Enterprise®, Visa would be able to consolidate consumers' userid/password pairs into a single secure e-vault and auto-propagate this federated identity information across the Visa/YOUnite enabled network of participating online merchants.

---

## Summary

YOUnite's patent-pending technologies present a revolutionary way to securely distribute and control access to personal information with complete customizable permissions without having to store that information on a centralized server. This data can be personal information, such as name, address and phone number or it can be personal preferences and attributes, such as shirt size, favorite style of food and preferred choice of online electronics vendor.

YOUnite, Inc. believes that YOUnite Enterprise® and YOUnite Mobile® offer a tremendous opportunity for the credit card processing industry not only in terms of generating additional revenue streams, providing valued-added services to its customers and the credit card users, but also in terms of yielding significant improvements to fraud protection.

This document has presented just three use case scenarios that YOUnite, Inc. confidently believes will provide companies like Visa with new services and/or enhancements to existing systems. Deploying YOUnite technologies will facilitate a level of differentiation and competitive advantage over its competitors as well as provide residual revenue streams.

\*\*\*\*\*

YOUservice LLC, a California Limited Liability Corporation, was founded in 2004 by Mr. Anthony Siress and his business partner, Mr. Mark Fitzpatrick. In late 2004, they incorporated, and funded YOUservice LLC. YOUnite, Inc. was then formed in November 2006 for the purposes of developing the patent-pending YOUnite Enterprise® technology. YOUnite, Inc. is located in Mountain View, CA. YOUnite Inc., is a Delaware "C" corporation and is a wholly owned by YOUservice LLC. To learn more about YOUnite Inc., YOUnite Enterprise® or YOUnite Mobile® please visit [www.youniteinc.com](http://www.youniteinc.com).