Online Interactions Data Study Findings

2008
Table of Contents

Introduction 3
Online Proofing and Online Identity 3
Data Study Methodology 4
The Power of Cross-Industry Collaboration 5
Adding Online Data to the ID Network 6
Study Findings 6
Summary 7
Introduction

For many businesses, the Internet has become a mainstream channel for customer acquisition, financial transactions, low-cost customer care, and delivery of sensitive information. While the convenience, personalization and speed of online interactions have resulted in mainstream consumer adoption, these same interactions have created new and unique challenges for businesses. One of these challenges is the validation of identity assertions made in an online or faceless transaction.

For years, financial institutions, communication companies and government agencies have relied on advanced analytical techniques to verify, or “proof” identity assertions during enrollment for financial accounts and services. While the sophistication of analysis may vary by institution, the identity data itself is often some combination of elements including name, address, Social Security number (SSN), date of birth, and phone number.

The importance of identity proofing is evident in the 2007 Consumer Fraud and Identity Theft Complaint Data published by the Federal Trade Commission. An examination of this data highlights the fact that identity theft victims had their personal information used to open new credit card accounts 40 percent more frequently than used to gain control of existing accounts.¹

Strong proofing processes play a critical role in the issuance of credentials such as credit cards, passports or wireless phones. While these credentials are often authenticated prior to each transaction, the actual identity associated with the credential is only authenticated once during the initial proofing process.

Online Proofing and Online Identity

The continued growth of eCommerce has stimulated the need for channel-specific proofing processes. In fact, some top-tier financial institutions have reported that the attempted fraud rate for online applications can be up to 10 times greater than attempted fraud through other channels such as phone and mail. The trend is similar in eCommerce environments where total losses from online payment fraud have steadily increased over the last three years. While the fraud rate (fraud losses as a percentage of total revenue) has slowly declined during this time, eCommerce has continued to grow at 20 percent or more each year, resulting in a net increase in actual fraud losses.²

In addition to online retail transactions and credit-related applications, online proofing processes support the issuance of online credentials such as passwords, tokens, or device registrations. Once issued, these credentials may be used to perform financial transactions, transfer funds, access sensitive information such as healthcare records, or make profile updates such as changes to a home address or phone number.

While the anonymity of the Internet adds new dimensions of complexity to proofing processes, the online environment also supplies a rich source of unique identity information that does not exist in other communication channels. Recent research from ID Analytics demonstrates the power of gaining greater insight of identity risk by combining personal identity elements with online identity elements such as Internet protocol (IP) addresses, device fingerprint, email address, and IP geolocation data.

¹ 2007 Federal Trade Commission Report on Consumer Fraud and Identity Theft Complaint Data
² Cybersource 9th Annual Online Fraud Report, 2008 Edition
Data Study Methodology

By devising innovative solutions that link identity activity with sophisticated pattern recognition techniques, ID Analytics has forged an identity-centric strategy based on two important differentiators.

The analysis that incorporated online elements resulted in a fraud detection improvement of more than 27 percent over the analysis using only personal identity information.

One is an extensive, continuously updated network of identity-related information and events. ID Analytics’ proprietary ID Network® is the nation’s only real-time, cross-industry compilation of identity information. ID Analytics built the ID Network from the ground up, gathering a constant stream of input from Fortune 100 companies. By contributing more than five billion cross-industry identity elements, 10 million known frauds, and nearly a billion identity events evaluated, ID Analytics’ clients ensure the ID Network’s real-time ability to deliver reliable, high-resolution visibility into how an identity behaves across industries over time.

The other component of ID Analytics’ identity-centric strategy is a portfolio of Advanced Analytics™ that integrate and interpret the data. These Advanced Analytics analyze the ID Network’s data across industries and companies, linking activity to pattern recognition algorithms to deliver unprecedented, real-time visibility of identity risk at any point in the customer lifecycle.

ID Analytics recently partnered with top-tier financial institutions and eMerchants to study the effectiveness of adding online identity elements such as IP address, device fingerprint, email address, and IP geo-location data to the ID Network. The study included over 12 million records such as applications for financial accounts and retail purchases performed online. The analysis was performed on accepted and rejected transactions and included the eventual outcome of each event (i.e., which events were later found to be fraudulent.) The study focused on the impact of integrating personal and online identity elements when determining identity risk during online interactions.
The Power of Cross-Industry Collaboration

In performing this research, all records were first analyzed using only the personal identity elements in the ID Network. Then a second analysis was performed including the online identity elements. In both scenarios, each application or transaction was evaluated using ID Analytics ID Score®—Risk solution. ID Score—Risk accurately assesses the identity risk level of an individual at any point of customer interaction.

Figure 1 illustrates a case study based solely on personal identity elements. In this scenario, a new customer is enrolling for a financial account. Advanced Analytics interpret the relationships between the information supplied on the application and data from the ID Network. In this instance, the individual’s address is associated with three reported frauds as well as four phone numbers — including one that is linked to an invalid SSN. This identity graph is indicative of identity fraud due to the relationships between individuals with multiple and invalid SSNs sharing a single-family residence with multiple phone numbers.

The analysis then focused on the integration of financial services and eMerchant data in order to analyze suspicious identity activity across industries. For example, even within industries where an SSN is not an available identity element, links can be established based on name, phone number, and address which may indicate suspicious activity.

Figure 2 illustrates an activity linked to a “ship-to” address used in fraudulent online retail transactions. Over a two year period, this same address was linked to more than 30 applications for consumer credit. In this example, an eMerchant was able to gain cross-industry visibility into application velocity based on financial services data, a pattern indicative of identity fraud.
Adding Online Data to the ID Network

Once the identity events were analyzed based solely on personal identity elements within the ID Network, the online identity elements were introduced. Figure 3 illustrates an individual enrolling for a financial account online. In this example, the applicant has supplied his or her name, phone number, SSN, email, and address. An IP address and a device fingerprint were also captured by the financial institution.

The additional online identity elements were used to create linkages between identity elements that were previously unrelated. This “network-effect” highlights the fact that the device used to perform the enrollment may serve as a linking key used to highlight suspicious activity elsewhere in the ID Network.

Study Findings

Using the same set of records in both scenarios, the analysis that incorporated online elements resulted in a fraud detection improvement of more than 27 percent over the analysis using only personal identity information. For a large credit card issuer, this would equate to eliminating an incremental $5 to $10 million of annual fraud losses without increasing the review rate. For eMerchant transactions, the combination of online and personal identity elements demonstrates an opportunity to eliminate 50 percent of manual reviews without increasing risk. As a result, eMerchants can better focus review resources while reducing cancellation of low-risk orders.

This study confirmed the value of gaining an integrated, cross-channel view of identity intelligence that combines personal information with online identity elements.

For eMerchants, ID Score-Risk consistently isolated transactions that resulted in a chargeback in addition to orders that were ultimately rejected by the retailer. This highlights the opportunity to lower losses by increasing scrutiny on the transactions most deserving of additional review. In addition, these findings represent an opportunity to increase revenue by maintaining a positive experience for legitimate customers who have already placed an order.
Figure 4 demonstrates a chargeback case study from this research. While there are many intricacies to this example, a few key points express the significance of the findings: Transaction A occurred with the customer providing name, email and shipping address. The IP address was also captured as an element of the identity. The combination of name, email and address enabled linkage to an SSN and phone which were linked to a prior fraud at a separate address (Transaction B). The phone used in Transaction A was also tied to 17 people supposedly living at a third address, a single unit apartment. Finally, the address used in Transaction A was linked to three prior frauds and 34 additional people living in a single-family residence. Without the ID Network, no single merchant could have gained the level of identity intelligence required for a clear perspective of risk.

Summary

The ID Analytics Online Interaction Data Study was performed with the support of top financial services firms and leading eMerchants. The objective of the study was to assess the value of including online identity elements to detect identity risk in online interactions such as enrollments, applications and transactions.

In addition to isolating fraud within financial accounts and retail transactions, online interactions include identity proofing processes which are performed prior to issuing credentials used for online authentication. Brokerage firms, healthcare insurers, and online banking sites should evaluate their identity proofing processes and evaluate whether or not they could benefit from gaining a unique, cross-channel view of identity risk in order to manage the impact of faceless interactions while protecting the consumer experience.

ID Analytics is committed to understanding the complex information patterns that make up an individual identity. This study confirmed the value of gaining an integrated, cross-channel view of identity intelligence that combines personal information with online identity elements in order to raise the bar for identity intelligence solutions.

For more information on how ID Analytics solutions can benefit your organization, visit www.idanalytics.com or contact ID Analytics at marketinginfo@idanalytics.com.