



GOMEZPRO RESEARCH BRIEF

SEPTEMBER 20, 2005

Requesting Personally Identifiable Information (PII)

Five Current Approaches Within Online Application Forms for Financial Products

Jen Cardello
Vice President, Customer Experience Services
Watchfire GomezPro

Requesting Personally Identifiable Information

SUMMARY

With the significant increase in phishing and identity theft, users are understandably concerned about the security and privacy of their personal data. Because of this firms may experience increased abandonment of online processes that require PII — Personally Identifiable Information. One such high risk process is the online application form for financial services such as deposit accounts, credit cards and loans. The following research brief describes and illustrates five current approaches to PII messaging.

Users are increasingly becoming more vigilant about the use of their personal information. Requests for two specific pieces of PII are likely to concern users more than other pieces of information:

1. E-mail address (Privacy concern: Receiving unsolicited e-mails)
2. Social Security Number/Social Insurance Number (Security concern: SSN ending up in the wrong hands)

Before entering such data, cautious users will want to know:

- Why this data is being collected
- What will be done with it
- What will **not** be done with it

Unfortunately, many firms do not currently provide this information within the application form itself. They cite the following reasons:

- 1) This information is included in an overall privacy and/or security policy
- 2) Some of this information is included in an overarching Patriot Act statement
- 3) Too much information will scare away users

Requesting Personally Identifiable Information

Our examination of leading financial services sites uncovered five approaches to PII request messaging (listed in increasing order of assurance):

- 1) No messaging
- 2) Generic icon linking to value-free information
- 3) Generic icon linking to valuable information
- 4) Intuitively worded link to useful information
- 5) On-page explanation

Examples:

1) No messaging: NOT RECOMMENDED

With all the attention that identity theft is receiving, it is crucial to proactively communicate the firm's usage of PII. Expecting users to provide their personal information, without being informed as to its use, is not prudent (see Figures 1 and 2). Better to over-inform and provide alternate means of application than under-inform and risk process, site and/or firm abandonment.

Figure 1

Enroll in Internet Banking

Enter Your Information: Step 2 of 4

Personal Accounts

▶ **Card or Account Number**

Enter your U.S. Bank Check Card or ATM Card number, omitting spaces and hyphens. If you do not have a Check Card or ATM Card, you may enroll using your checking or savings account number.

▶ **PIN**

Enter your 4-digit PIN (Personal Identification Number) for your U.S. Bank Check Card or ATM card.

▶ **Social Security Number**

Omit spaces and hyphens.

▶ **Personal ID**

Your Personal ID will be permanent; please select it carefully.

Create a unique Personal ID number. Personal ID numbers include spaces or can be creative in familiar with.

▶ **Confirm Personal ID**

Re-enter your Personal ID

▶ **Password**

Create your own Password in length and character protection; we recommend a password.

▶ **Confirm Password**

Re-enter your Password

By clicking "Continue," you acknowledge that you have read and accept the [Expanded Account Access Agreement](#).

Figure 2

Online Account Access

This page is for customers who do not have a user ID or would like to link a particular account to an existing user ID. Not yet a customer? [Apply now](#) and see how we can help you get more from your money.

To access your account online, you must first enable the account for online access. Please enter the information requested below, then click **Continue**.

Social Security Number:

Account Number:

Zip or Postal Code:

OptionsLink Customers
Get started now by [activating your account](#).

CONTINUE

Requesting Personally Identifiable Information

2) Generic icon linking to instructions/definitions: NOT RECOMMENDED

Particularly frustrating are sites that squander well-placed communication functionality: Specifically, page-specific or context-sensitive messaging. If a user is compelled to click on an “information” icon (e.g., Question mark), it is unlikely that he’s wondering what a Social Security Number is or what he is being asked to do: “Please enter your nine-digit Social Security Number” (See Figures 3 and 4). Rather, he wants to know why this piece of information is being requested, if it is truly needed, how the information will be used or if there is an alternate means of applying that doesn’t require online submission of this data.

Figure 3

The screenshot shows a web form titled "Personal Information" with a progress indicator "STEP 2 OF 5". The form includes fields for Social Security Number, Number of Dependents, City of Birth, Mother's Maiden Name, Marital Status, Gender, and Date of Birth. A "Help" icon (a question mark in a circle) is located in the top right corner of the form area. An arrow points from this icon to a separate box containing a list of instructions for the user.

Figure 4

13. Click **Next Page**.
14. In the appropriate fields, type:
 - Social security number
 - Number of dependents
 - City of birth
 - Mother's maiden name
 - Marital status (click to select from list)
 - Gender (click to select from list)
 - Date of birth
 - Senior Foreign Political Figure (click to select from list)
15. Click **Next Page**.

Requesting Personally Identifiable Information

3) Generic icon linking to useful information: ACCEPTABLE PRACTICE

Users may avoid clicking on generic icons, such as question marks and “i”s, because they do not know what lies beyond (See Figures 5 and 6). Users cannot be relied upon to predict the destination of links. Intuitively named links that predict user questions and summarize the destination information can increase the likelihood that users will get the information they need instead of abandoning the application. For example:

- “Why do we need your Social Security Number?”
- “How we will treat your e-mail address”

Figure 5

Online Banking Enrollment

Bank of America is committed to keeping your information secure with our [Online Banking Guarantee](#).

Online Security Check

Your Internet browser meets our security standards.

Browser in use = Internet Explorer 6.0.

[See our requirements for securing your Internet browser through SSL.](#)

Quick Help

Use this page to start your Online Banking enrollment.

What do I need to know?

- To preserve the security of your personal information, the

Get Started

To enroll in Online Banking or Online Banking Business Suite, you must first have a Bank of America account. [Open an account](#). To get started with Online Banking, please complete the information.

State where your accounts were opened: Massachusetts [Change state](#)

Social Security Number (SSN) or Tax Identification Number (TIN): [I don't have an SSN or TIN](#)

SSN (xxx-xx-xxxx) TIN (xx-xxxxxxx)

Bank of America ATM or Check Card PIN: [I only have a credit card account](#)

(4-12 digits) [I don't have any Bank of America cards](#)

E-mail Address: [?](#)

(name@email.com)

Figure 6

E-mail Help [close window](#)

We require your e-mail address to send you important notices about the Online Banking service, privacy policy changes, and statement availability and when notifying you that responses to your customer service inquiries are available.

We do not sell or otherwise share your e-mail address or any other customer information with marketers outside Bank of America who may want to offer you their own products and services.

If you wish to change your e-mail address or if you would prefer not to receive marketing offers from Bank of America through e-mail you can make changes to your customer information in the Customer Service area of Online Banking.

Requesting Personally Identifiable Information

4) Intuitively worded hyperlink leading to useful information: RECOMMENDED

Users appreciate sites that respect their time. A simple technique to make a site more respectful of users' time is to intuitively name links so that users can decide if the link is worth clicking on before ending up on an undesirable page (See Figures 7-10). In the case of PII, contextual hyperlinks that clearly indicate the information they lead to let users know that you are predicting their questions and increase the likelihood that the wary user will click through if he has a doubt about providing PII. For example: "[Why are we asking for your Social Security Number?](#)"

Figure 7

Figure 7 shows a registration form with several fields: "Last Name on Home Phone Bill", "Social Security Number" (with a "SECURE" lock icon), "Date of Birth", "Security Word Hint" (set to "Other"), "Security Word", and "Re-enter Security Word". A red asterisk is next to the "Social Security Number" field. A blue hyperlink "Why we need this" is positioned below the "Social Security Number" field. A red circle highlights this link, and an arrow points from it to Figure 8.

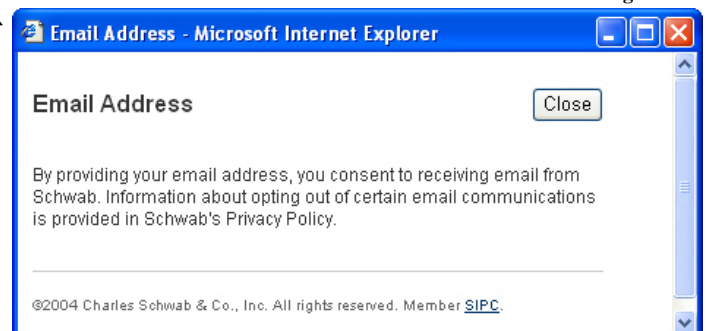
Figure 8



Figure 9

Figure 9 shows a registration form with an "Email address" field containing "test@testing.com". Below the field is a blue hyperlink "How we will use your email address". An arrow points from this link to Figure 10.

Figure 10



Requesting Personally Identifiable Information

5) On-page explanation: RECOMMENDED

If you have the space and can sum up your request in a few words without setting off the Compliance Alarm, then, by all means, inform users directly on the page. Ideally, this explanation should be located above, beside or below the field in question. If the explanation is located elsewhere on the page, it is likely to be overlooked.

Figure 11

Already signed up but don't see all your accounts online? [Sign on](#) and go to Add Accounts from the Account Services.

Social Security Number:

 Business Customers: Do not enter an EIN.
 I do not have a Social Security Number

ATM PIN:

 If you have a Wells Fargo ATM PIN for any of your accounts, please enter it.
 I do not have an ATM PIN

Account Number:

 Enter one of your Wells Fargo account numbers.
 (Account number not required if your only account is a student loan.)

Offer Code (optional)

Email Address:

 Your email address will allow us to contact you regarding your enrollment and use of this service.
 Yes, please keep me informed via email of new features, updates, and special offers at Wells Fargo.

Figure 12

Enroll [Help With This Page](#)

In this section, you'll create a User ID and Password.

- User ID and Password are case sensitive
- User ID and Password may not use the same letters consecutively ("AAA," for example)
- User ID may not match your password or Social Security Number
- User ID must be between 7-16 characters in length
- Password must be between 7-32 characters in length and must contain at least one number.

We request your e-mail address only for identification purposes unless you indicate you want to be notified by e-mail about special offers provided through Bank One. Read our [Privacy Policy](#) if you have any questions about how we use your personal information.

E-mail address:

Retype e-mail address:

Home Phone:

Business Phone:

Create a User ID:

Save User ID on this computer:

Create a password:

Retype password:

Requesting Personally Identifiable Information

Conclusion

Watchfire GomezPro encourages firms to test more explicit messaging via A/B testing and track user abandonment on a field-by-field basis. Specifically, firms should test versions of applications that utilize either on-page text or context-sensitive pop-ups to communicate:

- Why PII is being collected
- What will be done with it
- What will **not** be done with it

Currently, the number of firms proactively messaging the how's, why's and what-will-happen to PII are few and far between. However informative messaging is likely to become more prominent if firms begin to notice increased application abandonment or submission of bad data (fake e-mail addresses).