PLAID

The Power of Identity Sharing

Responsible identity data sharing can make both banks and consumers more secure

July 2017 | www.plaid.com

INTRODUCTION

As the financial services ecosystem matures, stakeholders have begun to consider — and implement — better approaches to safe and secure financial data sharing. And as these plans become more nuanced, many in the ecosystem are evaluating how best to handle account holder data fields, such as name, address, email, and phone number.

Like other pieces of data that consumers store at their bank, this information is sensitive and must be handled with care. But it's this data in particular that may prove critical to the continued development of the future of financial services.

The name, email address, physical address, and phone number comprise what we at Plaid call identity data. When combined with and checked across other data sources, each of these fields ultimately helps a consumer prove his or her identity.

Today, an array of digital services depends on this information — partly to prevent bad actors from accessing the financial services ecosystem, but also to deliver important services that hinge on knowing consumers are who they say. In the future, especially as the financial services ecosystem becomes even more interconnected, it's likely that such assurances will be even more important.

As such, identity info holds the potential to help protect banks, digital services, and consumers alike. That's why identity data sharing offers a rare example of a win-win-win: It increases security for banks, digital services, and consumers; lowers costs for financial institutions; and enables innovation for consumers.

Identity info holds the potential to help protect banks, digital services, and consumers alike

Financial institutions can do right by their customers — and critically, their own interests — by enabling measured identity data sharing with appropriate safeguards like consumer consent and the vetting by trusted intermediaries, which broker the data and technology connections between financial institutions, applications, and consumers.

FOUNDATIONS OF IDENTITY DATA EXCHANGE

While identity verification is important practically everywhere in the digital world, it's especially acute in online financial services. As with traditional offline finances, the digital ecosystem presents risks associated with money movement, which makes it important to know the identities of parties trying to access digital financial services.

As such, most financial services, digital or otherwise, need to validate their consumers' identities. Unfortunately, the concept of identity has also been one of the most stubbornly troublesome to digitize. As it stands, the onus remains on consumers to validate that they are who they say by supplying government-issued identification, such as passports or driver's licenses. In the digital world, consumers are often required to manually upload PDFs or email sensitive information like SSNs, passport and driver's license numbers for services to validate.

While a handful of solutions have attempted to translate identity verification into a friendlier online process, no consensus has been reached. Instead, we continue to rely on — and repeat — manual uploads and verifications.

But it need not remain this way. Consumers have identity information on file with their bank account — and financial services infrastructure is finally maturing enough to enable sophisticated sharing.

Consider the fact that, in order to open a bank account in the first place, consumers typically need to supply at least one form of government-issued identification, like a passport or state identification card. After the bank takes this consumer-supplied data and makes reasonable efforts to validate it, the institution often presents the information back to customers on their online account profiles and paper statements. Consumers frequently use these physical statements or PDFs to help verify identity or proof of address for other services.

Until recently, it wasn't possible to give consumers the opportunity to digitally port this information, because fintech infrastructure was immature. But today, trusted intermediaries like Plaid make it easy for consumers to choose to securely transport data, just as the healthcare industry has made strides toward portable medical records.

Today, trusted intermediaries like Plaid make it easy for consumers to choose to securely transport data, just as the healthcare industry has made strides toward portable medical records

In other words, rather than uploading a bank statement or utility bill that confirms name and address, a consumer can opt for a seamless and secure digital transfer by providing consent to port their bank-hosted identity info into other services.

USES OF IDENTITY DATA

Identity validation enables critical financial services for consumers. Although innovation is dynamic, core consumer financial activities that may depend on identity data include :

Validating ownership

Demonstrating ownership of a financial account is required for key activities like putting up collateral for a loan. For instance, in the mortgage space, lenders and other entities like government-sponsored enterprises require borrowers to verify ownership over a bank account associated with a mortgage application. Without the ability to digitally validate one's identity, consumers may be forced to manually upload and then email sensitive info to a mortgage lender or to submit a paper application. These methods are both less secure and less efficient than the automated digital alternative.

Establishing eligibility for critical programs

In the government space, some agencies are adopting digital tools that enable consumers to securely prove their identity. For instance, federal student loan programs may require a student to use identity info on file with a bank as an input for a loan application. Among other objectives, digital identity verification aims to reduce what some estimate to be more than $100 billion annually in fraud associated with government programs.

Permitting access to digital services

Many digital services need identity info to enable access to good actors and prevent access to bad ones. For example, an online brokerage platform vetting a potentialcustomer will need to verify that identity info associated with a customer's bank account matches the info on the brokerage account.

Enabling popular new methods of payment. One way to mitigate fraud and money laundering is for all links in the flow of funds to access critical info about the sender and recipient of funds, including identity info. Traditional payment methods -- like checks or wire transfers -- depend on this info exchange. Digital payment methods are already widely used by consumers, directly impacting banks. Banks can augment protections for these newer payment methods by allowing consumers to share their identity info.

"On the Internet, nobody knows you're a dog."

Given the shared priority of preventing "bad" access to the financial services ecosystem, it's worth taking a closer look at examples of how some specific digital services use identity info to limit fraud. The below chart illustrates the range of companies leveraging this information, which in many cases includes all four data fields available :

Identity data used to prevent improper access to the financial ecosystem and reduce fraud

Company Type	Use Case	Fraud Model
Payroll	Account linkage	Payroll companies collect identity data to match with user-inputted data to help ensure payroll funds are deposited in the earner's account and mitigate against payroll fraud, a common vector for money laundering.
Personal Financial Management (PFM)	Account linkage and funding	PFM tools leverage consumer-provided identity data along with data obtained from third-party databases to protect against fraudulent money transfers into or out of accounts.
Currency	Account linkage and funding	Many companies in the currency space have reduced fraud — in some cases by up to 5 times — by leveraging user-provided identity information to identify high-risk users for additional review.
Banking	Account linkage and funding	Banks leverage user inputs, consumer-provided identity information, and third-party databases to minimize fraud around new account opening and funding.
Financial Services	Payments	Many financial service firms compare identity data fields, info provided by a small business end user, and third-party databases within their own proprietary fraud algorithms that they adjust depending on risk tolerance.

DATA TRIANGULATION

It's important to note that none of the examples above uses data generated at a consumer's bank alone to validate identity.

After all, there tends to be little value in the raw account data itself; instead, it becomes a powerful part of the puzzle when the data is enriched and applied. Usually, services combine the data on file with the bank with other information, like data directly provided by a consumer or received from and/or confirmed with third-party databases.

This triangulation enables services to better prevent fraud (and other illicit activity like money laundering) when the puzzle pieces don't line up. Indeed, digital services — and the trusted intermediaries that connect them with financial institutions — employ sophisticated data science and risk-modeling teams to address this very issue.

Banks, too, often use this puzzle-piece approach to fight fraud. Whether processing a check, ACH payment, or wire transfer, banks seek to utilize all info at their disposal, including the names (i.e., identity info) of a payment originator and recipient. Sometimes this data is used to satisfy specific regulatory requirements, such as those imposed by the Bank Secrecy Act (BSA), Anti-Money Laundering (AML) rules, or the Office of Foreign Assets Control (OFAC). Other times, it's used to fight fraud more generally. Often, it's used for both: It reduces illicit activity while simultaneously meeting a regulatory requirement.

Across the ecosystem, combining identity data from multiple sources creates a more actionable view for digital services of the consumer in question. And triangulation and analytics can happen in near real time. Taken together, the whole greatly exceeds the sum of its parts.

Combining identity data from multiple sources creates a more actionable view of the consumer in question

The broader point is that digital services, whether fintechs or digitally enabled traditional institutions, want and need to use the best available set of tools to prevent illicit access and fraud. And all parties in the financial services ecosystem share the goal of keeping out bad actors.

OTHER PROPOSALS FOR DIGITAL IDENTITY

Some individuals have suggested that there are better options for digital identity validation. However, these alternatives have significant shortcomings compared to the controlled sharing of identity data enabled by trusted intermediaries, whose approach works today for millions of consumers with minimal effort required by bank partners :

OAuth and Tokenization

For example, some have proposed that tokenized authentication (e.g., OAuth), wherein a consumer logs in directly to their bank to enable a third-party service (rather than via a trusted intermediary), might eliminate the need for identity data exchange.

This is not the case.

Tokenization simply removes the need for user credentials to be used outside a bank for authentication; it doesn't actually verify a user's identity. In an OAuth flow, fraudsters could still use stolen credentials to access an account that doesn't belong to them.

Identity data on the account owner, however, can help solve this problem when combined with data obtained from other sources.

"Up-or-down" APIs

Other proposals would have banks create distinct APIs to validate identity data, which would function on an up-or-down basis. That is, the APIs would return a binary "yes" or "no" in response to a query whether "Jackie Smith" is a name attached to a particular account. (Some early industry efforts like Early Warning Services function on this basis.)

Most financial institutions don't have the resources or expertise to stand up identity APIs. For those that do, the up-or-down approach can be crude.

The algorithm behind an up-or-down API must be sophisticated enough to return "fuzzy" matches. It must determine that Jackie, Jacqueline, Jaclyn, Jack, and so on are all the same person (or not). The introduction of additional identity fields (i.e., name, email, address, phone number), typos, name and address changes, and more layer on additional complications. In other industries, the inability of up-or-down APIs to address this complexity tends to create false negatives, so that consumers who rightly should be approved for a digital service are rejected.

More important than their practical limitations, though, up-or-down APIs strip away transparency and put control in the hands of a consumer's institution, not the consumer. This can limit a digital service's ability to request and validate additional information, like secondary account owners, or use emails or phone numbers to perform two-factor authentication. This has significant implications, including undermining the ability to fight fraud.

Controlled sharing of identity data enabled by trusted intermediaries already works today for millions of consumers

---

ACCESS CONTROLS

Although consumer consent is a precondition for any type of data sharing, some skeptics have pointed to the privacy implications of this practice.

This focus on privacy is important: Banks, trusted intermediaries, and digital services all share incentives to protect the consumer's info. But identity data sharing does not mean granting unrestricted access to consumers' identity info to any third party; quite the opposite.

It's also important to bear in mind that this identity sharing already happens in the physical world: Consumers already share this information in printed or PDF form. The focus should be on how best to translate this activity to the digital realm — and thereby empower consumer choice. As is the case with other personal data, it's incumbent on stakeholders in the ecosystem to facilitate safe and secure ways for consumers to make use of their information. And in many cases, digital sharing is more secure than its physical counterpart.

To facilitate the digital sharing of identity info, **three** things should happen:

01 First, a financial institution or a trusted intermediary should conduct risk-based vetting of a digital service that wants to use identity information. This process includes, but is not limited to, reviews of the controls in place at the digital service as well as enhanced due diligence and ongoing monitoring based on risk profile and usage.

02 Second, a consumer grants a digital service consent to share identity info on his or her behalf. Even then, there should be contractually stipulated safeguards as to how the identity info can be used by digital services. Usage in line with the agreed upon safeguards and consumer consent should be protected, but violations should result in revocation of access.

03 Finally, a digital service should undergo regular audits and monitoring to evaluate compliance with encryption standards, security protocols for rate monitoring and limiting, and other processes like automated internal control reviews.

Ensuring privacy is an important shared priority, much in the way that preventing fraud is. However, practices are already in place that mitigate these concerns.

CONCLUSION

Identity data sharing is a high-stakes topic for the future of digital financial services — and that's why it's so important to get it right. Like other pieces of data a consumer stores at a bank, identity info is a sensitive set of elements that should be treated as such.

Banks can thoughtfully consider this sensitivity, balancing the need for identity data to protect consumers with measures to confirm that this data is used responsibly. Trusted intermediaries can help bridge the gap between these two goals by collecting consumer permissions and enforcing access controls on digital services.

Indeed, all layers of the digital financial services "tech stack" — financial institution, trusted intermediary, digital service, and consumer — have a role to play in safeguarding info and fighting fraud. All parties should aspire to a data-sharing ecosystem that balances innovation and consumer needs against security. By working together, including thoughtful sharing of identity data, the ecosystem can be even more effective in pursuit of this crucial shared goal.

Visit https://plaid.com/
to learn more