OLIVER WYMAN

POINT OF VIEW

SEPTEMBER 2017

THE EQUIFAX DATA BREACH
AND ITS IMPACT ON IDENTITY VERIFICATION

AUTHORS

Paul Mee

Chris DeBrusk

MARSH & McLENNAN COMPANIES

DOES THE EQUIFAX DATA BREACH MEAN THAT EXISTING PROCESSES FOR CONFIRMING THE IDENTITY OF CUSTOMERS NO LONGER WORK?

Equifax, a leading US credit bureau, has announced that it suffered a data breach resulting in the exposure of critical personal and financial data for 143 million Americans. The implications for the affected consumers are profound. While their credit cards can be re-issued with new numbers, their legal names, addresses, social security numbers, and birthdates cannot.

Equally profound are the implications for companies who use information stored by credit bureaus as a mechanism for confirming the identity of new and returning customers. At many companies, standard procedures for confirming customer identity involve asking for the "last four" digits of a social security number (SSN). The safety of this procedure is now in question and it is reasonable to assume that all these SSNs are now in circulation among fraudsters and for sale on the dark web.

Other standard procedures for confirming identity require the consumer to answer challenge questions based on the content of their credit files. For example, a consumer may be asked whether or not they took out an auto loan during the last six months; and if so, for what type of vehicle. Or, they might be asked to confirm a prior address. These methods are now far less safe as the underlying information has been hacked. In fact, there is a real question as to which commonly used identity-confirmation processes are still viable.

Banks, mortgage companies, insurance companies, asset managers, telecommunication companies, medical and health companies, hospitals and other organizations hold critical information on their customers, and often their money. These organizations arguably have a moral and fiduciary obligation to prevent fraudsters from obtaining data and using it to takeover accounts or open new accounts fraudulently. If organizations fail to protect their customers, they will expose themselves to legal action as well as potentially punitive responses from regulators.

In this challenging new world, we see three imperatives for chief risk officers, chief security officers, heads of compliance and line of business leadership.

SOCIAL SECURITY NUMBERS SHOULD BE CONSIDERED PUBLICLY KNOWN

Arguably, the safety of using SSNs in authentication has been declining for some years. However, the last four digits of the SSN are still casually assumed to be confidential information in identity verification processes. Companies need to start relying on information that is truly only known to the company and its customer.

PROCESSES FOR CONFIRMING CUSTOMER IDENTITY TO PREVENT ACCOUNT TAKEOVER AND FRAUD NEED TO BE RETHOUGHT

When considering fraud risk, and procedures for avoiding customer account opening or takeover by fraudsters, the use of third-party information for identity confirmation is now arguably much less reliable than ever before. Adapting to this new reality will complicate many existing processes, especially those that support account password resets because if a customer cannot access his or her account, you cannot readily confirm identity using past transaction history (unless the customer has a really good memory!).

The only information that can be used with confidence for identity confirmation is that which is unique to the consumer and the verifying company. A statistical approach could be taken that relies on a broad range of different types of information, the totality of which is unlikely to be available to a fraudster. However, given constant announcements regarding data breaches, even this approach could be challenged, especially in light of ongoing innovation by fraudsters and other bad actors.

Another complexity and practical challenge is that many organizations only encrypt and protect key data items such as SSNs in their systems, and don't protect the information that they will now need to use to confirm identity. A comprehensive reevaluation of what information is deemed "sensitive and critical" across databases and customer support systems needs to be performed and the means determined to protect this information from leakage or unauthorized access.

Today, many organizations use two-factor authentication as a mechanism to protect against account takeover attempts, phishing, and other fraudulent activities. The most common approach is to leverage a customer's mobile phone and a text message to confirm identity. It is worth noting that the information that was likely released in the Equifax breach (and others) could also be in use supporting identity processes by mobile phone companies.

Using text messages has always been of dubious merit. Mobile phone companies have themselves had difficulty preventing fraudsters from getting control of their customers' phones. Given the Equifax breach, the use of text messages to support two-factor authentication processes needs to be re-examined and alternative approaches implemented.

One potential new tool that companies can leverage to confirm identity are biometrics, although their use as a primary mechanism to confirm identity is still in question given the numerous examples of mobile phone fingerprint readers being spoofed by fakes. Emerging capabilities to perform facial recognition and iris scanning via mobile phones are worth watching to see how they can be leveraged — but won't address immediate challenges of confirming identity.

ACCURATELY IDENTIFYING NEW CUSTOMERS JUST GOT A LOT MORE DIFFICULT

Possibly the most difficult part of authentication takes place when a new customer opens an account. For complex financial products, this can be less of a concern due to the larger quantities of information that need to be collected, extensive know-your-customer processes and the sheer amount of time that opening a new account requires. Yet, as more and more consumer account opening processes are digitized and the time-to-first-transaction decreases, companies need to redesign the processes by which they confirm that the new customer truly is the person they claim to be. This is going to be even more critical for products that allow a customer to establish an immediate liability such as a short-term loan, or aim to provide an immediate service for a deferred payment.

Industry organizations such as the FIDO Alliance are attempting to create industry-wide standards and support new solutions to the identity problem. This is all to the good but in light of the Equifax data breach, it is imperative that each organization perform a comprehensive audit of its own customer identity processes to ensure they understand where changes are needed, and also that they are accurately assessing the risks of process failures.

Given the increasing sophistication of attackers, the question is more likely "when," not "if" you will be attacked and compromised. Too often organizations focus on the potential for direct losses (fines, litigation and remediation) that result in a customer account being compromised, and not enough on the reputational damage (impact on brand value and customer loyalty) that can result from being inadequately prepared for a major incident or data breach.

With these factors in mind, senior executives need to be asking the questions, **"Are we fully prepared to respond to a large scale information breach?"** and **"How do we protect our customers in the best possible manner?"**

ABOUT THE AUTHORS

Paul Mee
Partner in the Digital and Financial Services Practices
paul.mee@oliverwyman.com

Chris DeBrusk
Partner in the Finance and Risk, Corporate and Institutional Banking (CIB), and Digital Practices
chris.debrusk@oliverwyman.com

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

www.oliverwyman.com

OLIVER WYMAN