CIO
FROM IDG

How 3 fintech startups are shaking up security

By Bruce Harpham
CIO | Aug16, 2016 3:35 AM PT

Over the years, the financial industry has invested heavily in staff, processes and technology to improve security. But some startups are taking a more innovative approach.

Today's financial technology startups ("fintech" for short) are taking on some of today's greatest security challenges. Armed with drive and a need for innovation, these companies have created new services and security approaches that are changing the financial industry. Here's how three such companies are competing based on security.

Know your client

Proving personal identity is a key component of security for the financial industry. Most major financial institutions require customers to open accounts in person, present government-issued identity documents and wait hours or days to open an account. But customers today expect faster services — including the account opening process.

[Also on CIO.com: Threat geography: Why certain kinds of cyberattacks come from certain places]

Founded in 2010, Vancouver, British Columbia-based Trulioo, whose customer base includes well-known technology firms such as eBay, Kickstarter, Square and PayPal, has pioneered a new approach to verifying identity. While financial institutions typically rely on a small handful of identity documents, Trulioo uses a wider variety of data sources to verify identity, including property files, utility data, credit histories, watch lists, national health numbers and direct marketing data. This allows the company to issue a "verified" or "not verified" rating in seconds.

"The core information we verify are name, address, ID number and date of birth (i.e., DOB) – attributes which are core to KYC [know your client] compliance – but also extend to phone and email," says Trulioo CEO Jon Jones. "We customize the data sources for each client's situation: in some cases, a data source may require an ID number to be provided to access but the client may not capture that information so the source is not applicable, in other cases they may want a strict multi-source rule configured which means we need to incorporate several vendors, in other cases they may require a single-source rule where we can configure a waterfall approach to roll from data source to data source to minimize cost."

"The growing demand for KYC and compliance expectations mean it is important to have a high degree of confidence regarding customer identity," Jones says. "The next frontier for us to is make greater use of nontraditional data sets to verify identity such as customer payment records."

Password reuse (the good kind)

“Authentication is a burden to the user,” says Andre Boysen, chief identity officer at Toronto-based identity and authentication provider SecureKey Technologies.“An early insight for us was to segment password management into a spectrum. On one end, you have high velocity passwords like online banking that are used daily or weekly. At the other end of the spectrum, there are low velocity passwords such as online tax services that are used annually,” Boysen says. For example, each year, millions of people go to the Canada Revenue Agency (CRA) website to check on income tax returns, so access is important. Yet, the vast majority of users only access their accounts during income tax season.

SecureKey’s solution lets CRA users sign in with their bank user ID. “In contrast to many online services and accounts, bank account IDs are verified through an in-person inspection of identity documents and other means. That’s why it makes sense to use these IDs in other situations such as accessing online government services,” Boysen says.

Passing demanding government requirements for security is part of the SecureKey approach. “We go through Government of Canada audits twice per year and continue to be used by the government,” explained Dmitry Barinov, CTO at SecureKey Technologies. “We also use protocols such as Security Assertion Markup Language (SAML) and OpenID Connect in our products to enhance security,” Barinov said.

Protecting payments

Delivering payment services, especially across borders, remains an expensive and slow process. “At present, most banks do not have the infrastructure to support instant payments,” says David Schwartz, chief cryptographer at Ripple. Founded in 2012 and headquartered in San Francisco, Ripple seeks to deliver instant, certain, low-cost international payments. Ripple’s customer base includes Germany’s Fidor Bank AG and Earthport, a payment service provider.

“Many attacks on payment systems today focus on breaking into the system and entering false payment items,” says Schwartz. “Our approach is to provide cryptographic proof for each payment. This approach means that users can track payment status and misuse is much more difficult,” Schwartz says.

“Every account on the Ripple consensus ledger has up to three public keys associated with it. First, there is a master public key that proves ownership of the account. Second, we have a regular public key that can sign normal transactions. Finally, the third key is a message key that’s used to attach messages to transactions that only the account can read. Typical transactions have to be signed by either the regular key or the master key,” says David Patterson, director of corporate communications at Ripple. “Digital signatures can use either ECDSA SECp256K1 or Ed25519 and Schnorr signatures,” he adds.

Ripple is also reviewing ways to reduce its security management burden by adjusting information gathering processes. “One interesting recommendation that we got from a third party audit was to reduce the amount of information we log. There’s a tendency to log everything in case you need it, often with the idea that you can turn the auditing down later if it turns out not to be needed. A glut of data can reduce the amount of history you can keep, discourage analysis of the data and hurt performance,” Patterson says. ■