JUL 27
Jenna McNamee

Data privacy concerns will limit fraud detection technology

Article

The news: Many financial institutions have developed powerful technology to identify suspicious transactions and attempted money laundering. But some countries' information-sharing laws, along with customers' reluctance around data sharing, prevent the culprits from being caught sooner, per the Wall Street Journal.

Powerful technology: A number of countries have developed strong fraud and money laundering detection platforms, including the UK, the US, Estonia, and the Netherlands, per the Future of Financial Intelligence Sharing (FFIS) project, sponsored by UK think tank Royal United Services Institute.

For example, one platform currently in progress in the Netherlands allows a network of five banks to pool together encrypted data about customers.

- The platform can identify unusual transaction patterns and generate an alert while keeping customer data anonymous.
- While no data on the results has been released, the platform reportedly sent over 2,000 alerts to the respective banks for further investigation.

The creators of the platform, Transactie Monitoring Nederland, believe that pooling information will allow banks to identify patterns and trends they wouldn't see separately. And Dutch regulators agree, saying the platform cut down the time they spent following a web of money-laundering transactions from three weeks to two days.

Strict regulation: One caveat to the platform: It only works for business clients. That's because the data privacy laws for individuals in the Netherlands are much stricter than for businesses, making it difficult for banks to share customer data legally. The head of FFIS, Nick Maxwell, says the main obstacles are pre-existing legal frameworks. He says that governments need policies that explicitly pave the way for further information-sharing initiatives.

Varying sentiment: Many parties are involved in data sharing, and each approaches the topic differently.

Regulators

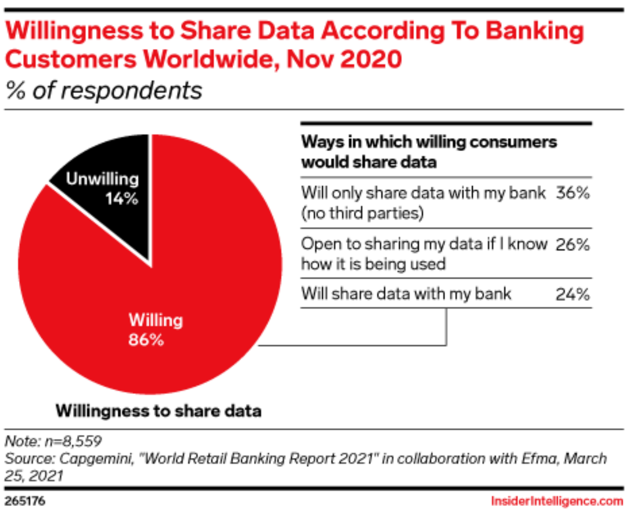
- In the US, banks can legally share customer data for the purpose of identifying money laundering activity and fraud via **The USA Patriot Act**, but participation is voluntary and there hasn't been much uptake. And the Consumer Financial Protection Bureau (CFPB) has been slow to enact mandatory data-sharing rules due to concerns the data may be exploited by Big Tech.
- In the UK, advanced open banking infrastructure has made it easier for banks to share data with each other, but only at a customer's request.

Banks

- In competitive banking markets in both the US and the UK, banks are less willing to share data voluntarily because they often deem it to be proprietary. They believe that sharing customer data will allow competitors to steal their customers.

Consumers

- Bank customers indicate they value fraud detection and prefer to bank with institutions with strong fraud detection programs in place. Yet consumers are wary about how their data is shared, especially with fintechs and other third-party providers that may aid in fraud detection.



Our take: Bank fraud and money laundering are important issues in today's digitized banking space. Fraud is surging in the UK, and regulators are cracking down on money laundering at many major banks. Technology seems to be the answer in combating bad actors. But the privacy concerns that come along with data sharing outweigh the benefits of the technology, at least when it comes to bank profits, consumer protection agencies, and the consumers themselves. As a result, sadly enough, these technological advances might never reach their full potential.


Companies Reporting Increased* Fraud Attempts by Industry According to US Business/Finance Executives and Security Professionals, Oct 2020
% of respondents
Insurance 75%
Banking 68%
Ecommerce 66%
Fintech 61%
Lending 53%
Prepaid 50%
Other 29%
Note: *vs. the prior year
Source: IDology, "Eighth Annual Fraud Report," Jan 28, 2021
263454
eMarketer | InsiderIntelligence.com