CROSS CHANNEL FRAUD INTELLIGENCE

Fraud detection often focuses on preventing unauthorized account access and transactions by an external party, which could occur due to account takeover, stolen credit card information or other fraud schemes. Many financial institutions implement detection tools to detect fraud in a given product or channel. However, managing fraud based on a payment product or channel rather than at the customer level can increase the potential impact of synthetic identity fraud, as the synthetic identity may have different types of accounts and payment products. In addition, analysis at the data attribute level (e.g., a Social Security number submitted in the application) may help identify additional synthetic identities, as data attributes often are reused across multiple relationships.

COMPONENTS FOR CREATING A CROSS-CHANNEL APPROACH

PRODUCTS

Criminals attempt to gain access to credit products (such as loans and mortgages) to quickly bust out or wait for credit limits to increase (such as for credit cards). Fraudsters apply for checking and savings accounts to gain entry and establish a relationship with a financial institution, using the accounts to move stolen funds and support their criminal activities. Once an account is opened, these criminal rings typically keep the account in good standing with regular transactions and leverage credit offers. It is important to look across the portfolio to identify all relationships the potential synthetic has at the organization.

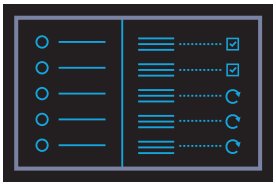
CHANNELS

Both consumers and criminals find it convenient to submit applications electronically through desktop and mobile channels. Required authentication steps and documents vary by financial institution. Organized crime rings often seek the easiest path to approval and avoid providing government-issued identification. However, based on the availability of fake credentials, fraudsters open accounts and apply for credit at bank branches if they believe the chance for approval is greater. Some crime rings repeatedly apply for credit using multiple channels to increase their likelihood of gaining approval. From each application submitted, criminals learn about approval thresholds, requirements, and both technical and process gaps that may be exploited. Fraudsters also gain knowledge through phone and chat customer service channels, where customer service representatives address inquiries and provide information. It is important to be aware of risks associated with each of the channels.

CROSS CHANNEL FRAUD INTELLIGENCE

CONSUMER DATA

When an application is received, a data attribute review can determine if there is a match to any known data associated with "bad actors," including whether some of the data attributes are used in other relationships. For example, a Social Security number may be associated with a different name, which could indicate a synthetic identity.



FRAUD INTELLIGENCE

Financial institutions can leverage tools and information across products and channels to detect synthetic identity fraud. Fraud intelligence refers to the use of data to mitigate fraud risks through detection. Whether institutions identify synthetic identity fraud during the application process, existing in the portfolio or after a default, those details can be added to "negative lists" to ensure details are not being used in existing relationships or are not reused in the future. Confirmed fraud cases can help build synthetic profiles to improve fraud detection based on risk scoring and activity patterns. Machine learning may help process the volume of data and produce alerts for review.

CONCLUSION

Synthetic identity fraud can be challenging to detect based on the nature of the threat and the fact that there is typically no consumer to identify and report the fraud. However, potential impacts of synthetic identity fraud are too great to ignore. Criminals are highly motivated to commit this type of fraud because of the financial incentives and high likelihood to avoid detection. As this type of fraud grows, related fraud losses, operational costs and reputational risks also increase. Identifying intelligence to detect fraud insights across products and channels can help mitigate the risk of synthetic identity fraud.