DATA STRATEGY FOR REPORTING SYNTHETIC IDENTITY FRAUD

THE IMPORTANCE OF REPORTING AND TRACKING SYNTHETIC IDENTITY FRAUD

Many fraud experts estimate that synthetic identity fraud is one of the fastest-growing financial crimes in the United States. While financial institutions of all sizes are impacted, the scope of the issue is not clear due to inadequate reporting. Many synthetic identity fraud losses are not identified as such, causing them to be misreported as credit losses. More accurate identification and reporting of synthetic identity fraud would benefit financial services companies and the overall industry by ensuring greater visibility of fraud trends that in turn, can encourage more effective mitigation approaches.

PROTECT YOUR BUSINESS

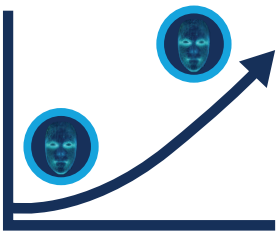
Financial institutions that can better detect synthetic identity fraud and categorize the fraud data are better equipped to mitigate potential negative business impacts. ***FiVerity estimates that synthetic identity fraud "bust outs" (maxing out a line of credit with no intention to repay) result in an average of $90,000 in theft.***

Crime rings often coordinate targeted synthetic attacks that continue until the activity is detected and mitigation implemented. When fraudsters are successful in busting out and stealing the maximum available amount, they most likely have established additional synthetic profiles with access to multiple credit products and other accounts that are building a positive credit history and preparing for the next theft. The criminals may attempt to expand the relationship by opening fake businesses based on established synthetic identities to obtain access to business loans and products, including merchant card processing services. These fake businesses can be used to establish more synthetic identities. An expanded financial relationship with access to higher credit limits often translates to a larger fraud loss at bust-out.

To help catch synthetic fraud, financial institutions can review all losses for credit products, such as loans and credit cards, along with losses from overdrawn accounts due to check fraud. Merchant services card processing losses also may be caused by synthetic identity fraud, which can be definitively determined after an in-depth review. For example, the collection process is an opportunity to identify whether an actual person or synthetic is responsible for the credit loss. This research step can be built into the collection process, with feedback provided to both the credit product and fraud detection teams. However, a review during the collection process may not provide the level of detail needed to identify synthetic identity fraud. Fraud or investigations teams may need to subsequently conduct a more thorough review to examine all the details of the applicant and the transaction history of the account prior to default.

DATA STRATEGY FOR REPORTING SYNTHETIC IDENTITY FRAUD

Increased knowledge about synthetic identity fraud potentially can help an organization prevent these types of fraud losses, decrease lending and operating costs and avoid the need for more restrictive lending rules. Tighter lending rules could cause a loss of potential customers and revenue, but not prevent the synthetic identity fraud. Furthermore, a failure to identify the scope of synthetic identity fraud losses may interfere with building a business case to fund improved fraud detection. In addition, the reputational impact of a large synthetic identity fraud loss event may cause a loss of potential and existing customers to flee if they do not have confidence in account security.



INDUSTRY IMPACT

The lack of accurate synthetic identity fraud reporting impacts the financial services industry. If financial institutions do not review credit losses to find synthetics, then the scope of the issue cannot be fully determined and addressed. Likewise, organizations cannot determine the true impact of synthetic identity fraud if they combine fraud reporting for traditional and synthetic identity fraud into one category. Synthetic identity fraud is likely to continue to grow if fraudsters can avoid detection and accountability. More broadly, lack of a reliable industrywide fraud loss total is likely to understate its scope and therefore, may discourage the industry from addressing synthetic identity fraud through information sharing to support detection, promote awareness and learning, and identify potential solutions. Undetected synthetic identity fraud is less likely to be reported to law enforcement or result in prosecution of the perpetrators.

INDUSTRY EXPECTATIONS

Financial institutions often review fraud losses to amass detailed data, learn from events and identify trends that can be used to improve fraud detection. This approach also can apply to credit losses to determine if losses are due to a bad credit risk and a failure to repay an obligation or should be categorized as synthetic identity fraud. Improved identification can benefit financial institutions, allowing them to enhance fraud detection, reduce fraud losses and potentially, prevent a large loss from crime ring activity. Accurately classifying and reporting the fraud to law enforcement is critical to ensure the perpetrators can be identified. Sharing fraud examples and event information with others in the financial industry can benefit other financial institutions and make it harder for crime rings to operate successfully.

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.