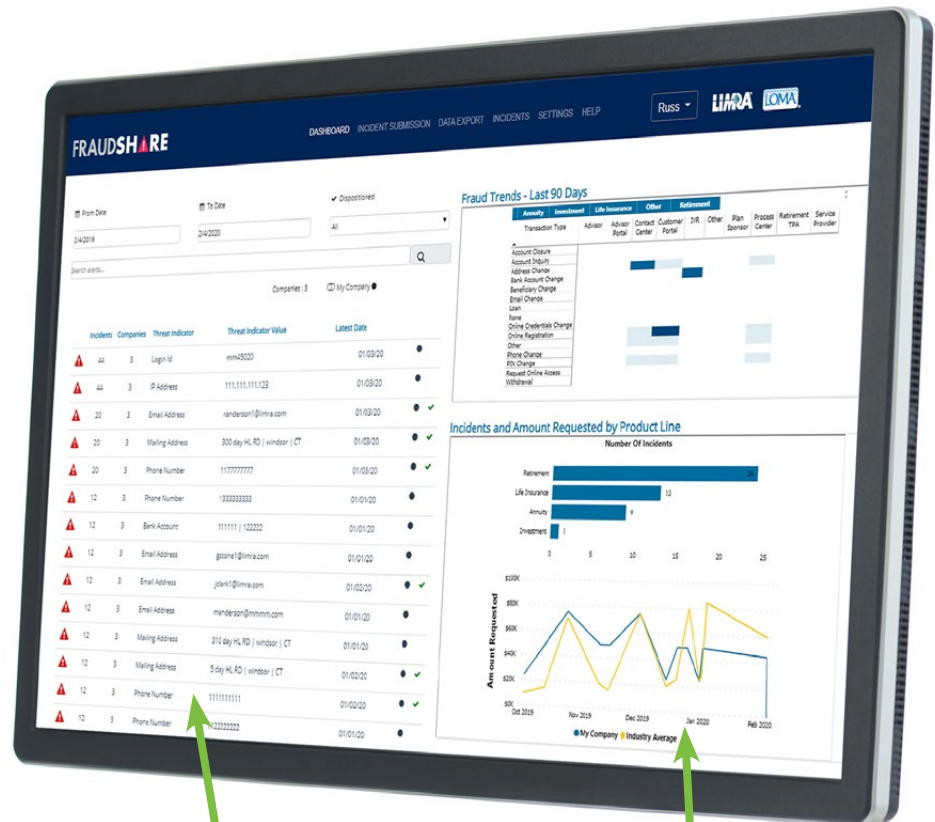


FRAUDSHARE

Used by Leading Companies Across the Financial Services Industry to Combat Account Takeover Fraud

- FraudShare enables companies to defend against account takeover (ATO) attacks perpetrated by unknown and unrelated third-party imposters.
- FraudShare provides easy and secure real-time access to incident data related to recent and ongoing ATO attacks.
- FraudShare provides the threat indicators associated with current and ongoing ATO attacks to help companies stop fraudsters at the gate.
- FraudShare provides additional intelligence to conduct more thorough ATO fraud investigations.
- FraudShare is uniquely positioned as one of the only industrywide ATO fraud information sharing applications to provide industry-level ATO attack metrics.



Easy access to the threat indicators used by fraudsters, showing how often and how many companies attacked

Provides industry-level incident data allowing companies to compare and contrast

Learn more about this secure, convenient, centralized, and timely early-warning system – and how to join a community of fraud fighters. Request a demonstration:

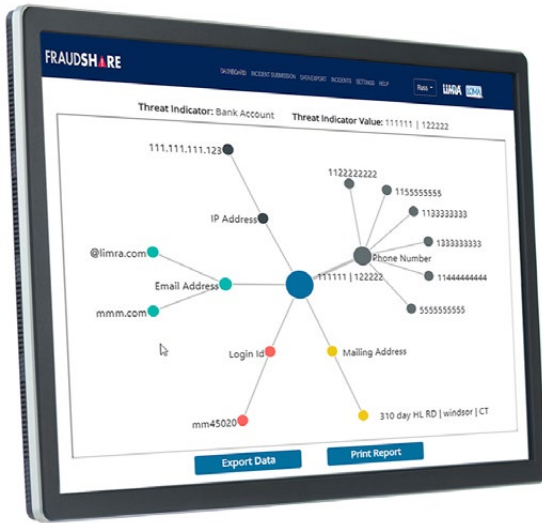
✉ FraudPrevention@limraloma.com

💻 www.limra.com/fraudshare **or** www.loma.org/fraudshare



FRAUDSHARE

The Neighborhood Watch for the Financial Services Industry



Understand and investigate ATO attacks with powerful correlation analysis tools showing relationship between threat indicators and incidents

The screenshot shows a detailed incident reporting form. It includes sections for 'Incident' (Product Line, Life Insurance, Group/Individual Product, Incident, Extension Type, Address Change, Access Point, Access Method, Fraud Scheme, Address Impersonation), 'Risk' (Request Disbursement Method, Total Account Value, Amount Requested, Detection Method), 'Phone' (Fraudster Incoming Phone Number, Fraudster Phone Number, Fraudster Callback Number), 'Email/Online' (Fraudster Email Address, Customer's email was compromised, Fraudster Login ID), and 'Address' (Fraudster AddressLine1, Fraudster AddressLine2, Fraudster City, Fraudster State, Fraudster Zip Code). There is also an 'Additional Details' section for 'Repeat Fraudster'.

Comprehensive incident reporting provides additional information to better protect against future ATO attacks

No company or customer data is exchanged

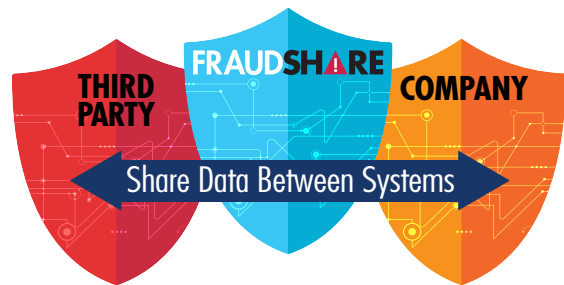
The screenshot shows an email notification from FraudShare. It includes a table with the following data:

Alert Level	Companies	Incidents	Threat Indicator	Threat Indicator Value	Latest Date	My Company	Disposition
Red	2	2	Phone	View Details	2/4/2020	Yes	Yes

Below the table, it says 'Please do not reply to this message'.

Companies can receive real-time email alert notifications or access the FraudShare data directly through data export capabilities or APIs

FraudShare works great as a stand-alone ATO fraud detection and prevention application, and even better when linked to a company's other fraud prevention tools and applications. FraudShare makes your fraud prevention program more robust and effective.



“FraudShare is a superior addition to our suite of fraud prevention tools. We are starting to see FraudShare identified as the detection method. As more companies are onboarded, the impact will increase. The tool provides an early-warning indication of potential suspect activity allowing John Hancock to proactively research and stop a potential account takeover, protecting customer assets.”

Laurene Polignone, AVP, John Hancock Risk Management

“FraudShare has been a great addition to support our fraud-fighting efforts. The integration has already helped Securian Financial prevent fraud.”

Scott A. Helgeson, Business Operations Director

“FraudShare helped us identify fraudulent calls that went undetected previously – effectively serving as a valuable early-warning system.”

Wondsossen Mezlekia, Symetra Operational Risk Manager

