

2018

TRANSUNION FINANCIAL SERVICES SEMINAR

Smarter Decisions: The Consumer First Era

Identity Management and The Evolution of Fraud in Lending

Antoni Guitart
Senior Director,
Fraud Analytics

Anne-Marie Kelly
Executive Director,
Identity Management





Notice

IN NO EVENT SHALL ANY STATEMENTS CONTAINED IN THIS DOCUMENT BE DEEMED LEGAL ADVICE OR LEGAL OPINION. IN ADDITION, NOTHING CONTAINED IN THIS DOCUMENT SHALL BE DEEMED TO CONSTITUTE A WARRANTY OR OTHER LEGALLY BINDING REPRESENTATION OR STATEMENT ON THE PART OF TRANSUNION, IMPOSE ANY LEGAL OBLIGATION OR DUTY ON TRANSUNION, OR OTHERWISE BE DEEMED TO REVISE, AMEND, OR OTHERWISE MODIFY ANY AGREEMENT BETWEEN TRANSUNION AND THE RECIPIENT OF THIS DOCUMENT (“RECIPIENT”) INCLUDING, IF APPLICABLE, BUT NOT LIMITED TO ANY AGREEMENT UNDER WHICH TRANSUNION HAS DEVELOPED AND/OR DELIVERED THIS DOCUMENT.

COMPLIANCE WITH ALL LAWS IS SOLELY THE RESPONSIBILITY OF THE RECIPIENT. THE RECIPIENT IS ADVISED TO CONSULT ITS OWN LEGAL COUNSEL TO DETERMINE ITS OBLIGATIONS UNDER APPLICABLE LAW.

NO PART OF THIS PUBLICATION MAY BE REPRODUCED OR DISTRIBUTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR OTHERWISE, NOW KNOWN OR HEREAFTER DEVELOPED, INCLUDING, BUT NOT LIMITED TO, THE INTERNET, WITHOUT THE EXPLICIT PRIOR WRITTEN CONSENT FROM TRANSUNION.

REQUESTS FOR PERMISSION TO REPRODUCE OR DISTRIBUTE ANY PART OF, OR ALL OF, THIS PUBLICATION SHOULD BE MAILED TO:

**LAW DEPARTMENT
TRANS UNION OF CANADA, INC.
3115 HARVESTER ROAD, SUITE 201
BURLINGTON, ON
L7N 3N8**



In this session, we'll discuss:

- Core features of consumer credit fraud for lenders
- Synthetic fraud use case
- Areas of focus for fraud management in the current environment
- TransUnion's new approach to Identity Management

Fraud management has a broad impact across the organization; it's not only about financial loss



AREAS OF IMPACT



REGULATORY

- Know-Your-Customer Programs
- Watch list Screening
- Anti-Money Laundering



FINANCIAL

- Fraud-based default losses
- Operational costs of fraud prevention programs



REPUTATIONAL

- Customer loyalty
- Marketplace image

A further complication stems from the diversity of fraud behaviors affecting lenders

Third-party fraud:
Individual consumer targeted and victimized

Account takeover

Unauthorized transactions on a victim's account, obtained through malware or phishing, data breach or physical interception

Identity theft

Obtaining new credit by misappropriating a victim's identity, obtained through a data breach or a victim's intercepted personal records

First-party fraud:
No consumer victimized

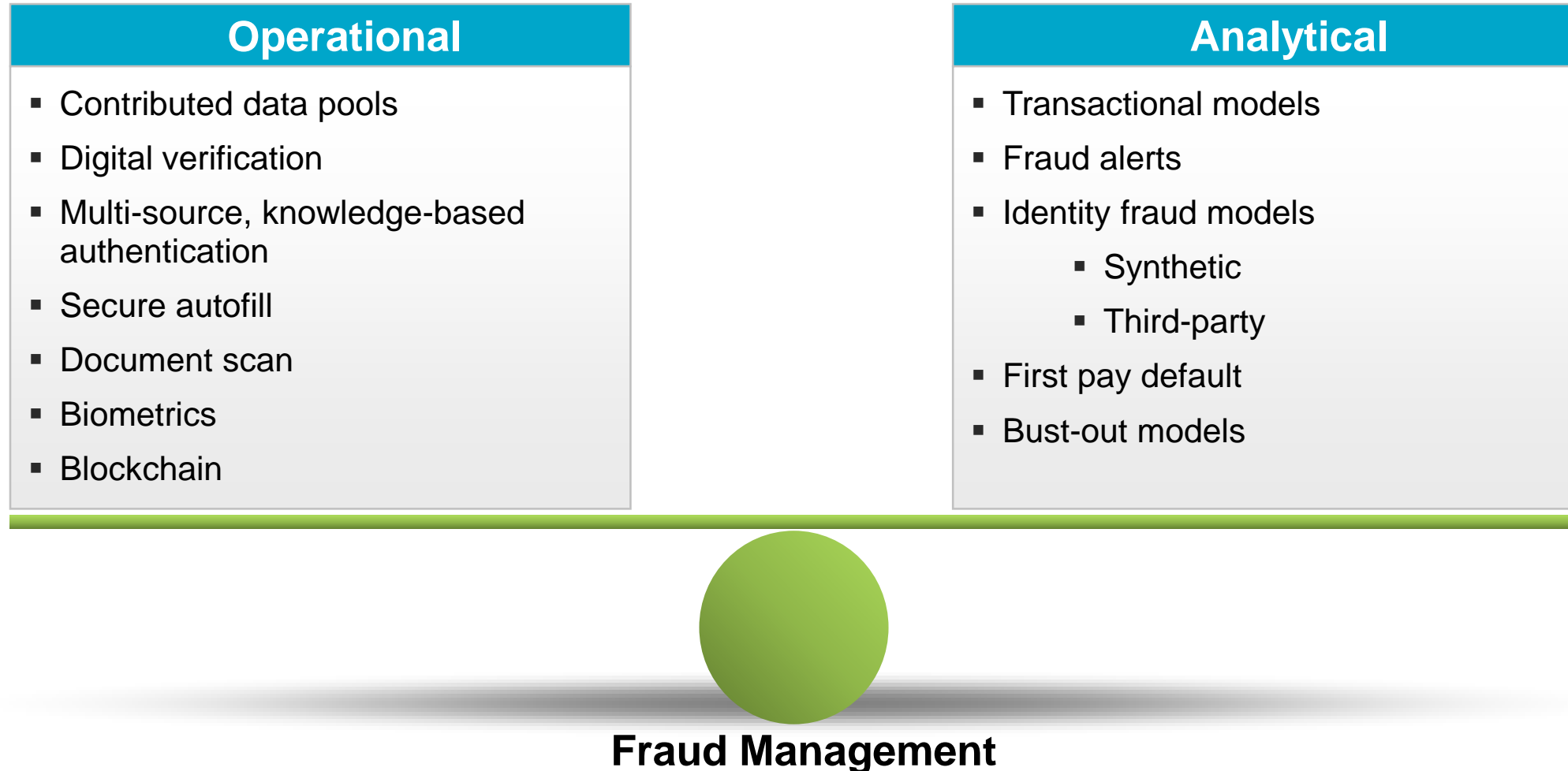
First pay default

Obtaining new credit with no intent to honor contractual obligations

Synthetic identity

Using a fictitious identity that is manufactured with real and fake personal information to build a credit profile over time, often ending in default

Addressing these threats requires lenders to balance a mix of fraud prevention tools



Fraud is creative and evolving by nature, often times in response to significant systemic shocks

Impact on fraudsters

Impact on lenders



Move to digital

- Enables high throughput
- Lowers exposure upon detection
- Exploits lender focus on frictionless customer service

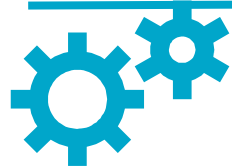
- Creates a vital but high-risk channel
- Requires a secondary source of authentication around the device rather than just identity



Data breaches

- Cheap access to millions of PII, financials, and passwords on the dark web
- Fuels quasi-algorithmic fraud

- Exponentially increases the size of the fraud threat on lenders
- Operational cost: fraud prevention, added info security friction



Structural shifts

- Push fraudsters further into remote fraud schemes
- Crowding out of transactional card fraud

- Diminishes opportunities for counterfeit card fraud (EMV, mobile wallet)
- Manage secure environments

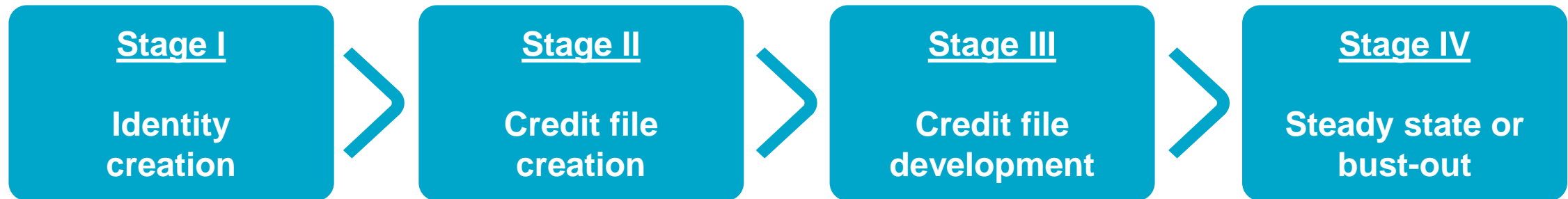
Synthetic fraud has become a rising concern because of its size and growth. It also provides a valuable illustration of the complex and evolving nature of fraud.

The creation of a synthetic identity involves a phased approach, although its end purpose can be diverse



Synthetic Identity Fraud: Creating a fictitious identity from disparate PII and building a credit profile over time, for the purpose of credit fraud, credit repair or credit creation

PHASES OF SYNTHETIC IDENTITY CREATION



SYNTHETIC IDENTITY USE CASES

FRAUD

CREDIT REPAIR

NEW CREDIT FILE



The mechanism used by a synthetic identity can best be illustrated by real, high-loss cases

	Q1-2014	Q2-2014	Q3-2014	Q4-2014	Q1-2015	Q2-2015	Q3-2015	Q4-2015	Q1-2016	Q2-2016	Q3-2016	Q4-2016	Q1-2017	Q2-2017
VantageScore® 3.0	751	699	631	708	695	566	745	670	733	548	332	347	396	457

NEW ACCOUNT OPEN SEQUENCE

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

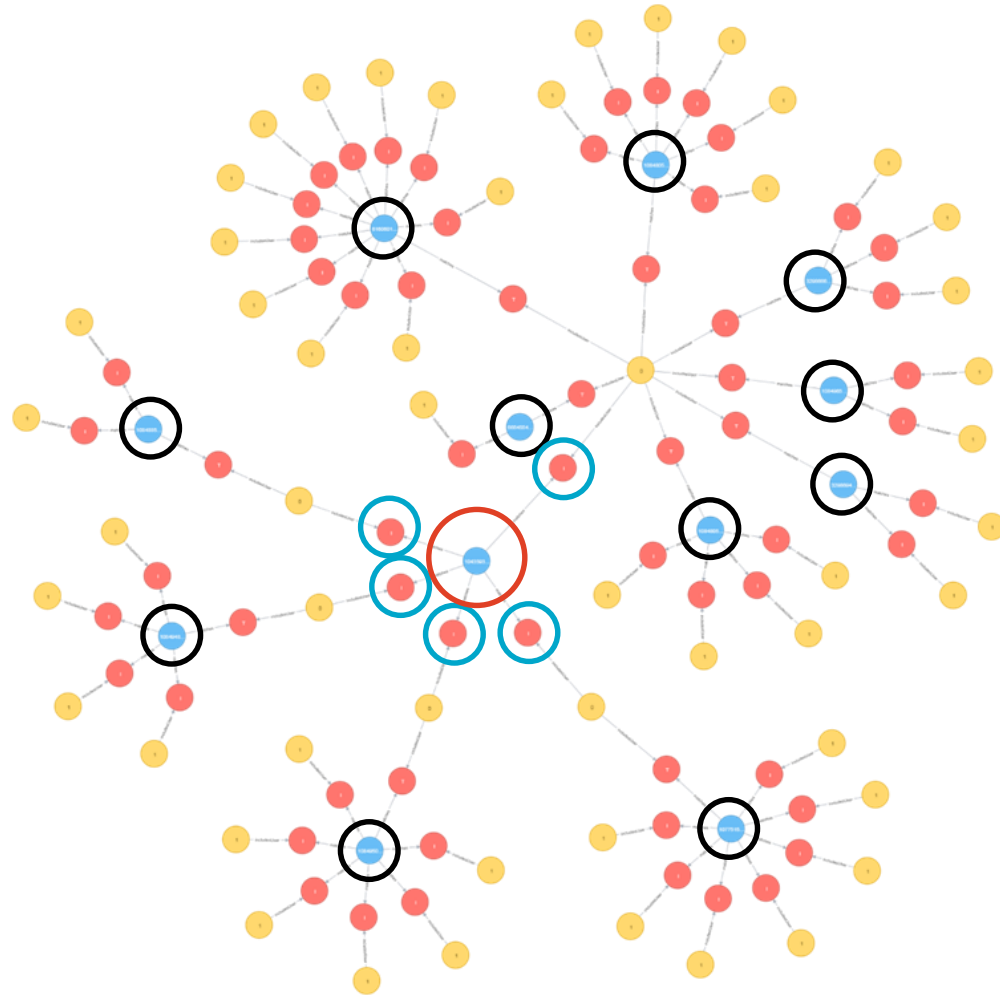
A ()	Authorized user trade opened (# of associated users)
O	Individual trade opened
C	Account closed
CBG	Account closed by credit grantor
X	Charge-off






Charge-Off Amount

STAGE 1 - CREATE FILE | **STAGE 2 - MATURE** | **STAGE 3 - BUILD ACCESS** | **STAGE 4 – BUST-OUT AND EXIT**

Source: TransUnion consumer credit database

Individual cases can be staggering, but a network view highlights the systemic nature of the problem



-  Breeder consumer
-  Breeder accounts
-  Synthetic consumers
-  Synthetic accounts
-  Synthetic charge-offs

- We start with a single breeder on 5 card accounts
- 11 new identities created using authorized user accounts
- 47 new, primary credit accounts are established
- All accounts in the network go to charge-off
- Total network loses: \$364,000



We observe clear trends in our consumer database that help identify synthetic identity risk and credit file creation

		<u>Synthetics</u>	<u>Non-synthetics</u>
SSN REPORTING VELOCITY	Median time difference in months between SSN first reported date for SSNs shared across consumers	6	281
ADDRESS SHARING WITHIN 6 MONTHS	Median number of consumers reporting a given address for the first time within 6 months	20	0
AUTHORIZED USER AS FIRST TRADE	Percentage of consumers for whom the first trade is an authorized user	66%	8%
SHARED AUTHORIZED USER ACCOUNTS	Percentage of consumers who share an authorized user account with 4+ other consumers	61%	0.2%

Synthetic classification based on TransUnion's internal investigations

Source: TransUnion consumer credit database



The power of these models is magnified rather than diluted, as we measure it within specific risk tiers

Bankcard early pay default rates – synthetic score by VantageScore® 3.0

		TRANSUNION SYNTHETIC FRAUD SCORE						Total
		901-1000	801-900	701-800	601-700	501-600	100-500	
RISK TIER	SUPER PRIME	38.0%	33.7%	16.0%	2.7%	0.9%	0.2%	0.2%
	PRIME PLUS	32.0%	27.3%	8.7%	2.0%	0.8%	0.5%	0.5%
	PRIME	30.0%	21.6%	6.2%	2.2%	1.6%	1.2%	1.3%
	NEAR PRIME	31.0%	23.0%	6.6%	3.6%	4.0%	4.1%	4.1%
	SUBPRIME	37.5%	27.3%	13.8%	9.1%	9.2%	13.0%	12.8%
	Total	32.1%	25.3%	7.9%	3.3%	2.8%	3.0%	3.0%

Sample of originations from 2013 through 2017
 VantageScore® risk tiers: Subprime:300-600; Near Prime: 601-660; Prime: 661-720; Prime Plus: 721-780; Super Prime 781-850
 Early Pay Default defined as 60+ DPD in 6 months

Source: TransUnion consumer credit database

TransUnion recognizes the need to evaluate synthetic evidence on multiple dimensions

Consumer view



What are the factors within the **matched consumer credit report** that indicate high fraud risk?

- Usage of authorized user tradelines
- Recent credit seeking activity
- Timing of credit history build

Systemic view



What are the systemic factors within the **entire credit bureau and alternative data universe** that indicate high fraud risk?

- Sharing of PII elements
- Timing of PII sharing
- Address tenure



With a multi-dimensional view, we can effectively fine-tune our fraud mitigation strategies

Bankcard early pay default rates – Consumer by systemic synthetic score

		TRANSUNION SYNTHETIC FRAUD SCORE						Total
		901-1000	801-900	701-800	601-700	501-600	100-500	
SYSTEMIC SYNTHETIC SCORE	901-1000	41.9%	48.0%	39.7%	34.4%	31.6%	27.3%	40.3%
	801-900	38.9%	39.1%	31.2%	15.3%	7.7%	9.0%	17.8%
	701-800	41.8%	37.1%	15.3%	5.8%	3.2%	3.6%	5.7%
	601-700	26.8%	21.0%	7.6%	3.5%	2.2%	3.8%	3.6%
	501-600	19.1%	7.6%	4.7%	3.0%	2.0%	3.9%	3.3%
	100-500	0.0%	4.3%	6.4%	3.0%	3.4%	3.0%	3.0%
	Total	34.5%	28.8%	8.4%	3.2%	3.0%	3.0%	3.0%

Sample of originations from 2013 through 2017
 Early Pay Default defined as 60+ DPD in 6 months

Having explored the challenges of fraud, what else can be done to help address this evolving problem in the current environment?

We've identified four areas of focus that we believe can have a meaningful impact on fraud prevention

REAL-TIME DATA REPORTING

- Systemic impact of fraud requires coordinated systemic response
- Real-time data sharing increases operational hurdles for fraudsters

ANALYTICS

- Machine Learning methodologies are ideal to identify complex data patterns
- Explainable Artificial Intelligence approaches will prevent “black box” outcomes for fraud management

OPERATIONAL IMPROVEMENTS

- New technologies can lower fraud and lower friction, previously an unavoidable trade-off
- Secure auto-fill, biometrics, doc scan, blockchain

ALTERNATIVE DATA

- Incorporating life events and identity relationships to enhance identity view
- Getting an asset and geolocation footprint to measure transaction plausibility

Smarter Decisions:
Innovation in the Consumer First Era

The result is we need to think about identity management differently than in the past. Identity is key to much more than Fraud — it's the new, strategic battleground for financial services.