Consumer Identity Behaviors and Account Takeover

Paul Baer

Sr. Director, Head of Risk Solutions NA

Legal Notice

Disclaimer

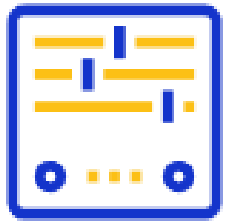
The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

All brand names and logos are the property of their respective owners, are used for identification purposes only, and do not imply product endorsement or affiliation with Visa.

Today’s discussion

What are consumer identity behaviors and account takeover?

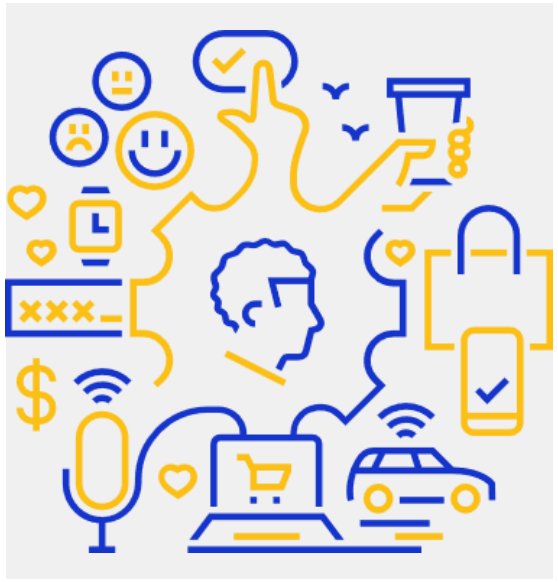
What is the issue and the impact?



What can we do about it?

What are consumer identity behaviors and account takeover?

What are consumer identity behaviors?



Use of features to build confidence around a consumer profile

Online retailers leverage a variety of attributes to evaluate risk, including:

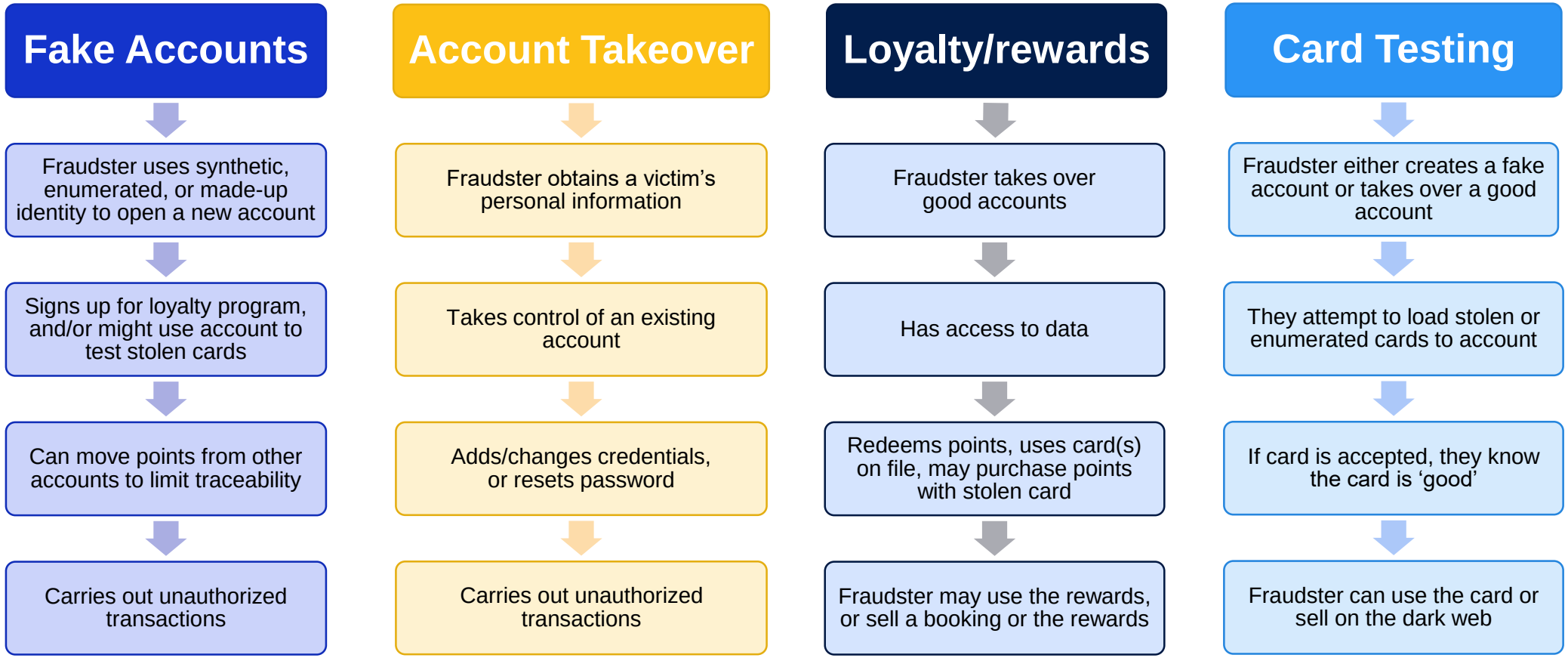
- Good/bad history associated with email addresses, payment instruments, and addresses
- Click and data entry patterns within a transaction session
- Biometrics (anatomical, physiological, behavioral characteristics)
- Patterns across transactions with time-on-page and device

Use of stolen consumer credentials to commit online fraud

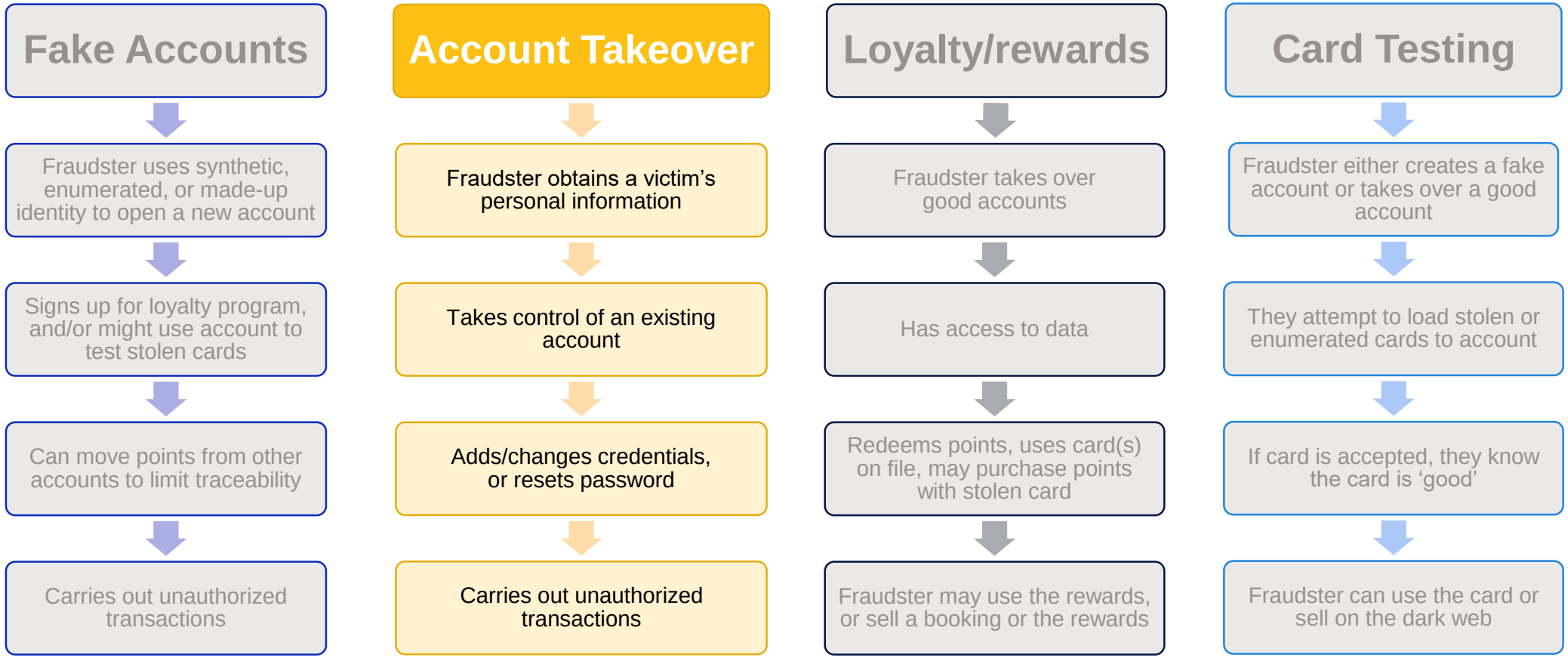
Fraudsters gain access to a user's online accounts and pose as real customers to:

- Make unauthorized purchases
- Steal loyalty rewards
- Leverage the stolen information to access other accounts
- Sell stolen information on the dark web

Different types of account fraud



Different types of account fraud



What is the issue and the impact?

Growing threat of account takeover and account-related fraud

Common forms include account takeover, loyalty fraud, and card testing

27%

of merchants globally are experience loyalty fraud putting customer loyalty rewards at risk

23%

of merchants globally experience account takeover

37%

of merchants globally experience card testing attacks

Source: 2022 eCommerce fraud report

Figure 17 – respondents were asked “Which of the following types of fraud attacks, if any, have you ever experienced at your organization?”

More entry points for account fraud than ever

How are people paying online?

Why is account takeover a growing risk?

- Fewer than six in 10 US digital shoppers pay online with a “traditional” credit card
- Apple/Google/Walmart/Samsung Pays can be integrated into merchant consumer wallets (with broad adoption in 18-34 demographic)
- Electronic wallets are being used by the demographics with the most spending power
- PayPal remains popular but has possibly peaked – and been replaced with Venmo

Which Payment Methods Have US Digital Buyers Used to Make Digital Purchases?	Female	Male	18-34	35-54	55-65	Total
Credit card	59%	60%	41%	64%	70%	59%
Debit card	57%	43%	57%	48%	45%	50%
PayPal	46%	50%	49%	52%	43%	48%
Gift certificate	24%	13%	15%	19%	21%	18%
Cash	16%	23%	28%	20%	11%	19%
Apple Pay	15%	22%	37%	15%	6%	19%
Buy now, pay later services	14%	9%	17%	11%	7%	11%
Venmo	10%	12%	20%	11%	4%	11%
Retailer app/account	9%	8%	12%	9%	5%	9%
Google Pay	8%	15%	17%	12%	4%	11%
Walmart Pay	6%	17%	20%	13%	2%	11%
Samsung Pay	2%	9%	10%	8%	0%	6%
Other electronic wallets	3%	5%	8%	3%	1%	4%
None	1%	0%	0%	1%	0%	0%
Other	2%	2%	1%	3%	2%	2%
Don't know	0%	0%	0%	0%	0%	0%

Data is from the October 2022 "The Insider Intelligence Ecommerce Survey" conducted by Bizrate Insights.

1,049 US adults ages 18 to 65 were surveyed online between October 2 and October 27, 2022.

Respondents identified as female (52%) and male (48%) and were ages 18-34 (32%), 35-54 (33%), and 55-65 (35%). Data has a margin of error of +/-3 percentage points at the 95% confidence interval.

"The Insider Intelligence Ecommerce Survey" conducted in Dec 2022 by Bizrate Insights, Dec 15, 2022

Layering consumer identity behaviors in risk strategies v1

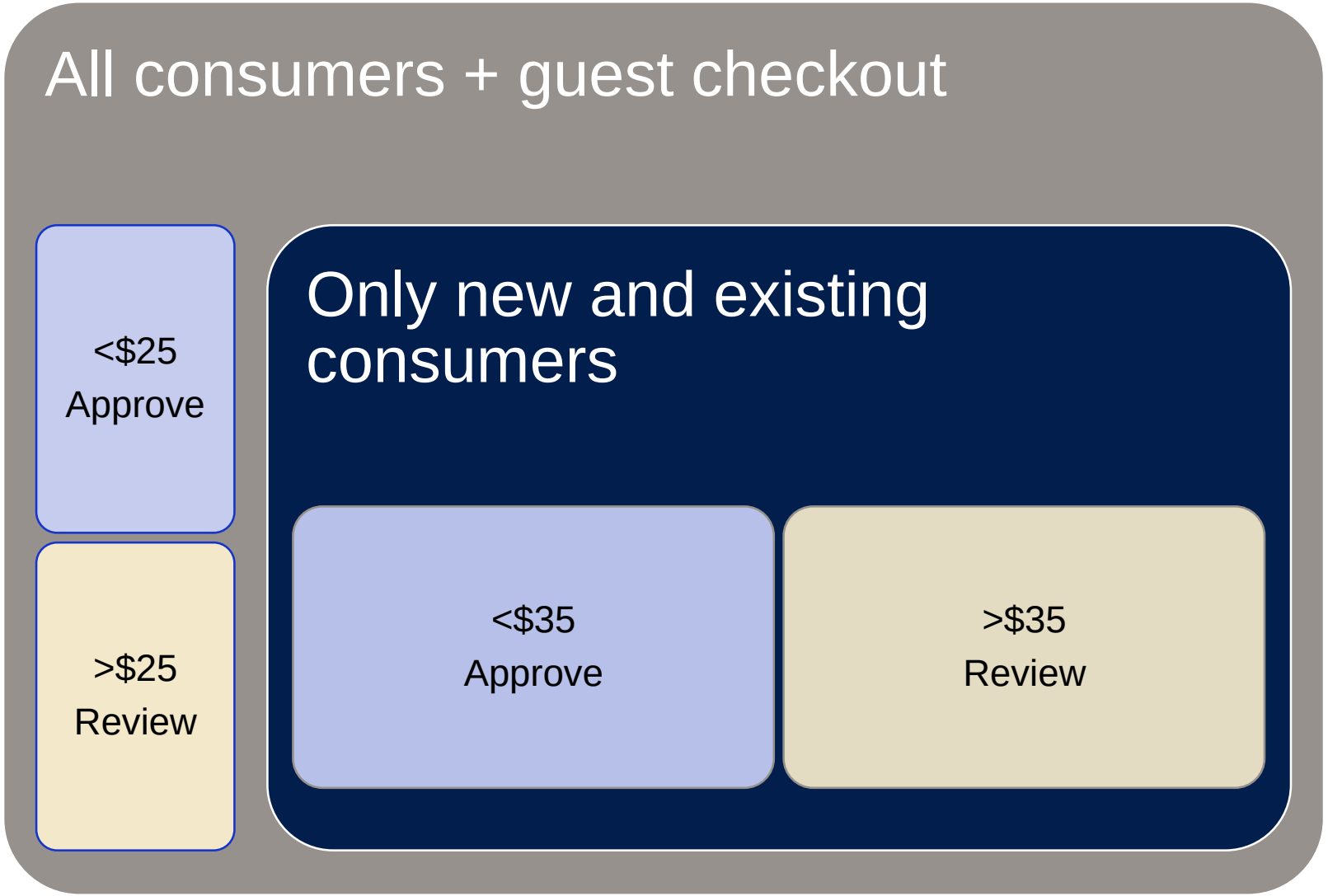
Increasing acceptance and reducing false positives

Merchants have more data on their customers than ever

Consider an ecommerce merchant

- Average ticket = $20
- Consumer account distribution
  - 45% are new consumers with an account
  - 45% are existing consumers with an account
  - 10% guest checkout

Segmenting guests from registered customers can allow for more automation



VISA

Strategies shared are for example purposes only and are not based on any merchant

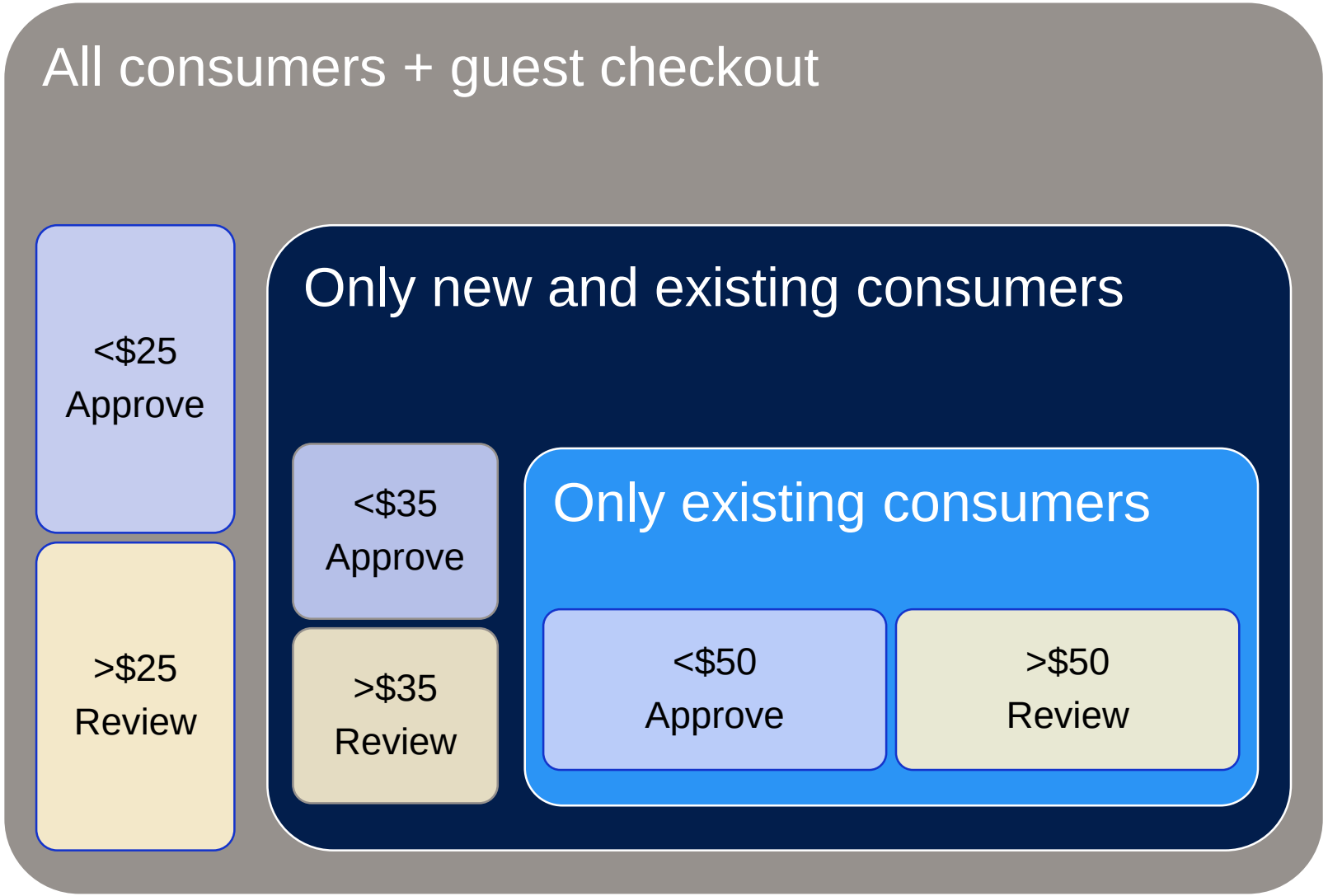
Layering consumer identity behaviors in risk strategies v2

Increasing acceptance and reducing false positives

Segmenting guests from registered customers can allow for more automation

Further groupings by new vs. existing customers can reward your loyal buyers and provide a better experience

But what about existing consumers who have changes on their accounts?



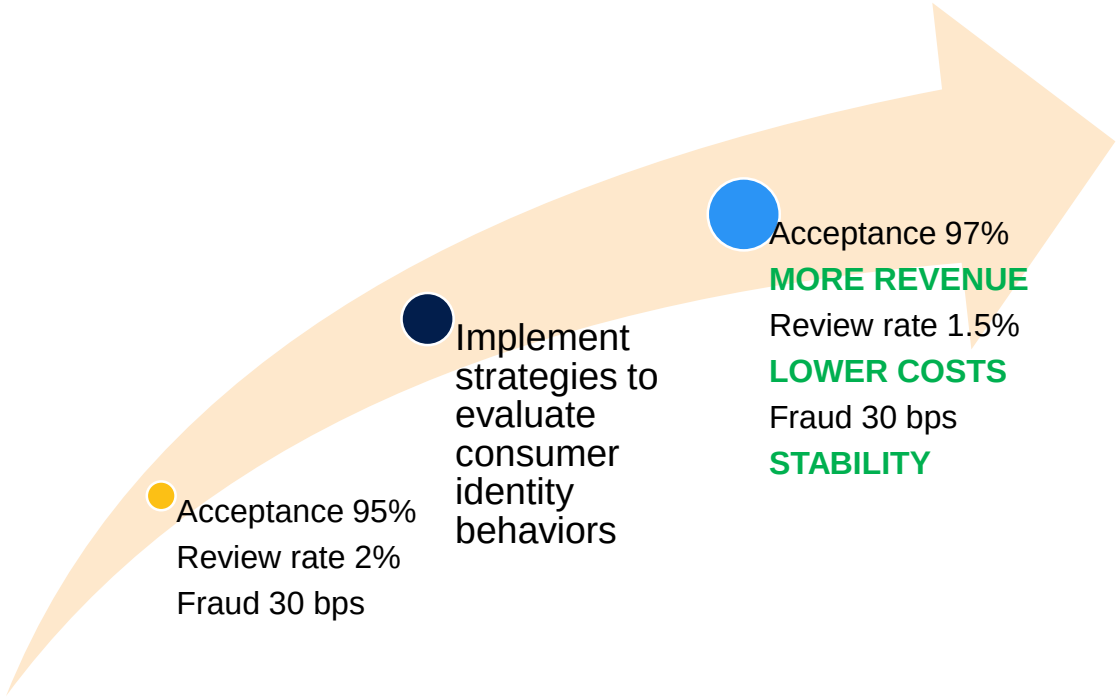
Strategies shared are for example purposes only and are not based on any merchant

Benefits outweigh the risks of using consumer identity behaviors…

…but there are still risks

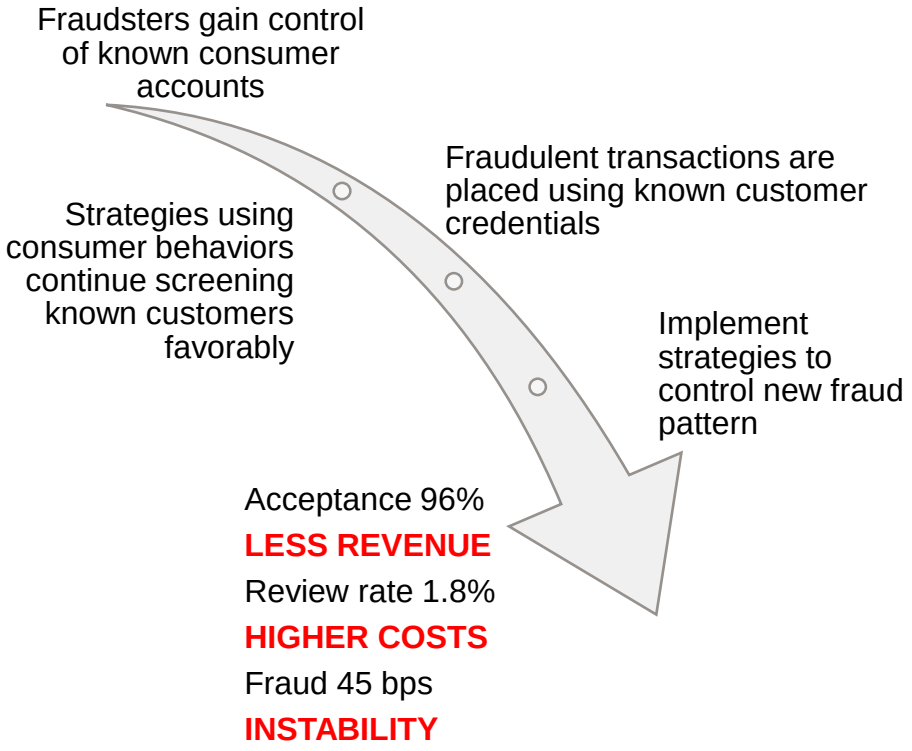
Simple example timeline

Begin using consumer behavior



Simple example timeline

Begin to see account takeover

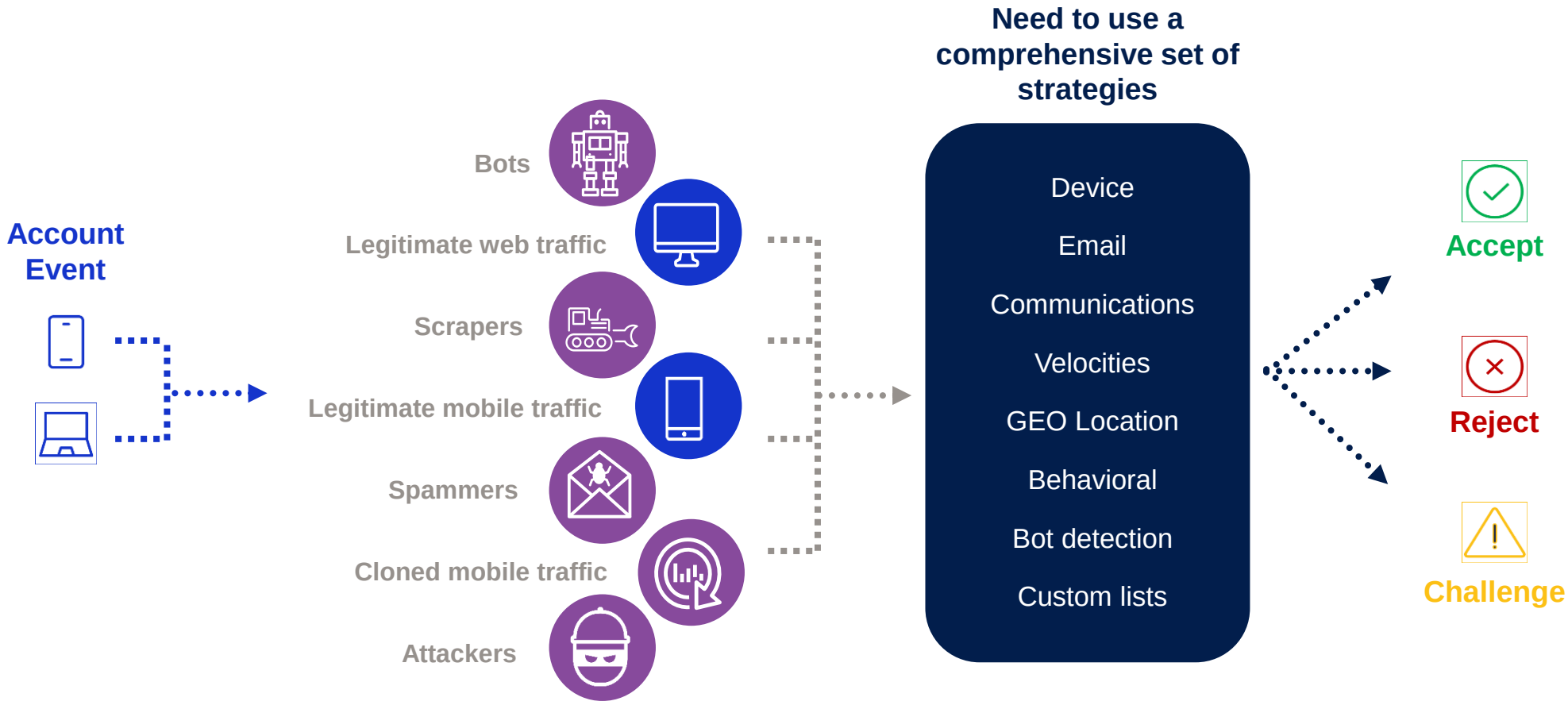


Acceptance and review rates shared are for example purposes only and are not based on any merchant

What can we do about it?

Risk tools can help

Identify good customers and block the bad requesters



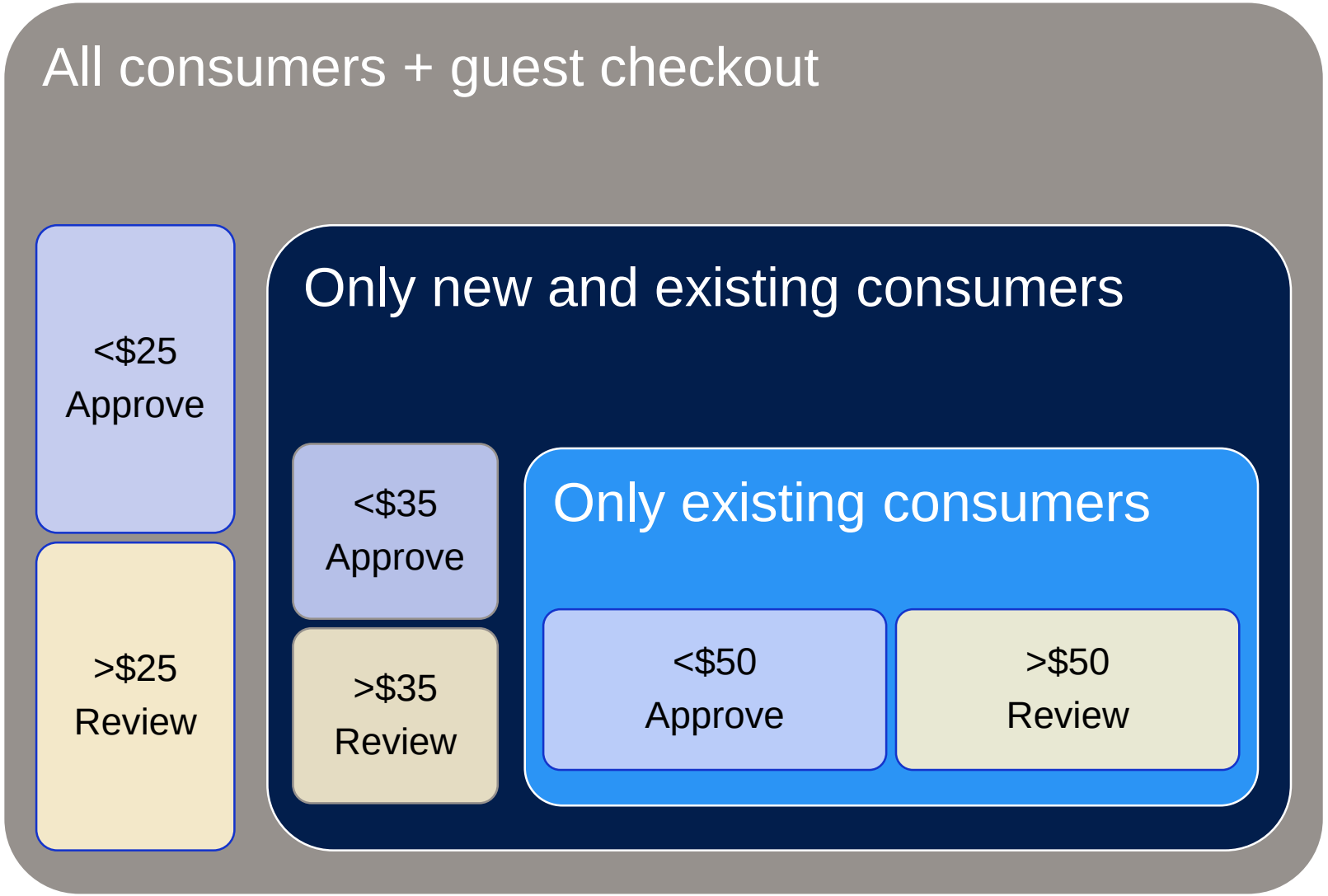
Layering consumer identity behaviors in risk strategies v2

Increasing acceptance and reducing false positives

Segmenting guests from registered customers can allow for more automation

Further groupings by new vs. existing customers can reward your loyal buyers and provide a better experience

But what about existing consumers who have changes on their accounts?



Strategies shared are for example purposes only and are not based on any merchant

Layering consumer identity behaviors in risk strategies v3

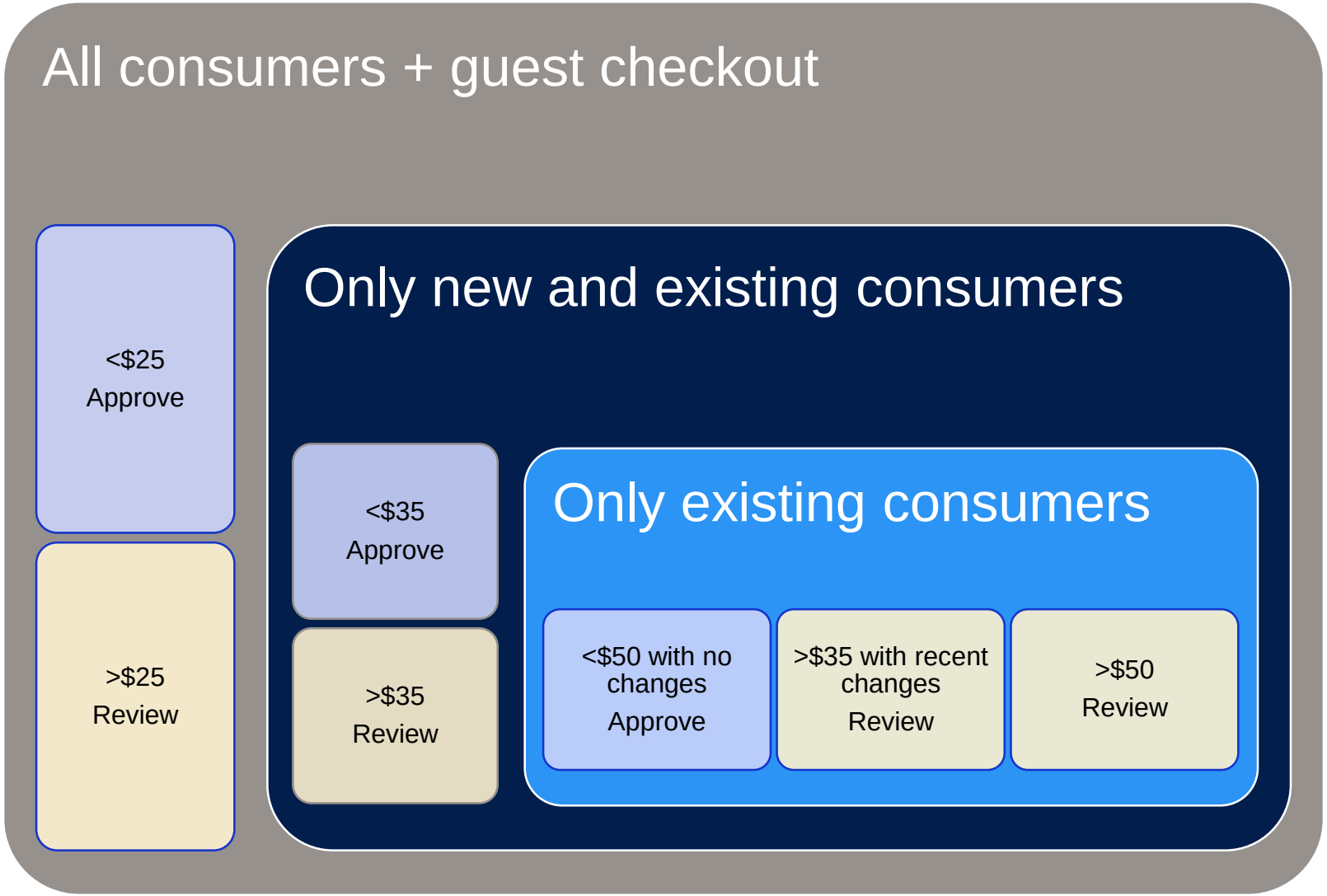
Increasing acceptance and reducing false positives

But what about existing consumers who have changes on their accounts?

Evaluating the stability (or instability) of various attributes on an account allows for differentiation across existing customers

Other ways to differentiate

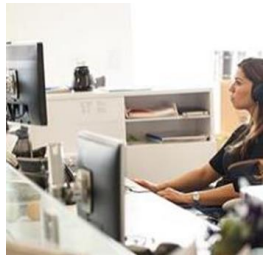
- Has a card been added that is already on multiple other accounts?
- Is the most recent purchase atypical for the customer?



Strategies shared are for example purposes only and are not based on any merchant

Key indicators of account-related fraud

Predictive attributes can help identify bad actors



Helpdesk/customer service calls reporting unauthorized account activity (i.e., escalations)

- Customers claiming someone has “taken over” an account
- Customers see unknown transactions on an account

Spike in card loading to accounts and associated fees (i.e., card testing)

- Abnormal number of new account creations (sometimes with synthetic identities)
- Charges for authorizations related to payment instrument add/update activity

Increase in account creation and management activities (i.e., changes in passwords, emails, etc.)

- Fraudsters using account holder credentials to make changes (email address, card on file, phone number)
- Unauthorized transactions from customers with positive history

A merchant reputation is at stake

Best practices for minimizing potential exposure

			
Intention	Avert fraud attempts before they happen	Protect online accounts from unauthorized access	Preserve customer trust and loyalty
Example actions	• Monitor velocities on account activities, usernames, email, device • Look for accounts with atypical changes	• Limit number of cards loaded per account • Alternate authentication methods (2FA, designated)	• Implement risk tools and adapt with changes • Balance good and bad user behavior to protect your brand

"It's imperative for businesses to have a mitigation strategy in place.
It's also critical to be proactive, particularly given the rapidly rising volume of e-commerce transactions in the wake of the pandemic.
Failure to do so can have negative financial implications along with loss of customer trust."

-Julie Conroy, Head of Risk Insights at Aite-Novarica Group

Thank You!

Resources

Account Takeover Protection
https://www.cybersource.com/en-us/atp.html

Search for account takeover on the Cybersource and Visa websites for much more!

Paul Baer
Sr. Director, Head of Risk Solutions NA
Visa Risk & Identity

https://www.linkedin.com/in/paulhbaer/