U.S. Credit and Debit Fraud Landscape

Bankcard Fraud Prevention Strategies Webinar

Carolina Gallegos
North America Risk Services
May 14, 2015

Notice of confidentiality

This presentation is furnished to you solely in your capacity as a customer of Visa Inc. and/or a participant in the Visa payments system. By accepting this presentation, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions contained in the Visa Rules and/or other confidentiality agreements, which limit your use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa Inc. or as a participant in the Visa payments system. The Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system. Please be advised that the Information may constitute material non public information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material non public information would constitute a violation of applicable U.S. federal securities laws.

Forward-looking statements and disclaimer

This presentation may contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms “objective,” “goal,” “strategy,” “opportunities,” “continue," “can,” "will" and other similar references to the future. Examples of such forward-looking statements may include, but are not limited to, statements we make about our corporate strategy and product goals, plans and objectives. By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance and (iii) are subject to risks, uncertainties, assumptions and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors, including the following: macroeconomic and industry factors such as currency exchange rates, global economic, political, health and other conditions, competitive pressure on customer pricing and in the payments industry generally, material changes in our customers' performance compared to our estimates; systemic developments such as disruption of our transaction processing systems or the inability to process transactions efficiently, account data breaches involving card data stored by us or third parties, increased fraudulent and other illegal activity involving our cards; and the other factors discussed under the heading "Risk Factors” in our most recent Annual Report on Form 10-K and our most recent Quarterly Reports on Form 10-Q. You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement, because of new information or future developments or otherwise.

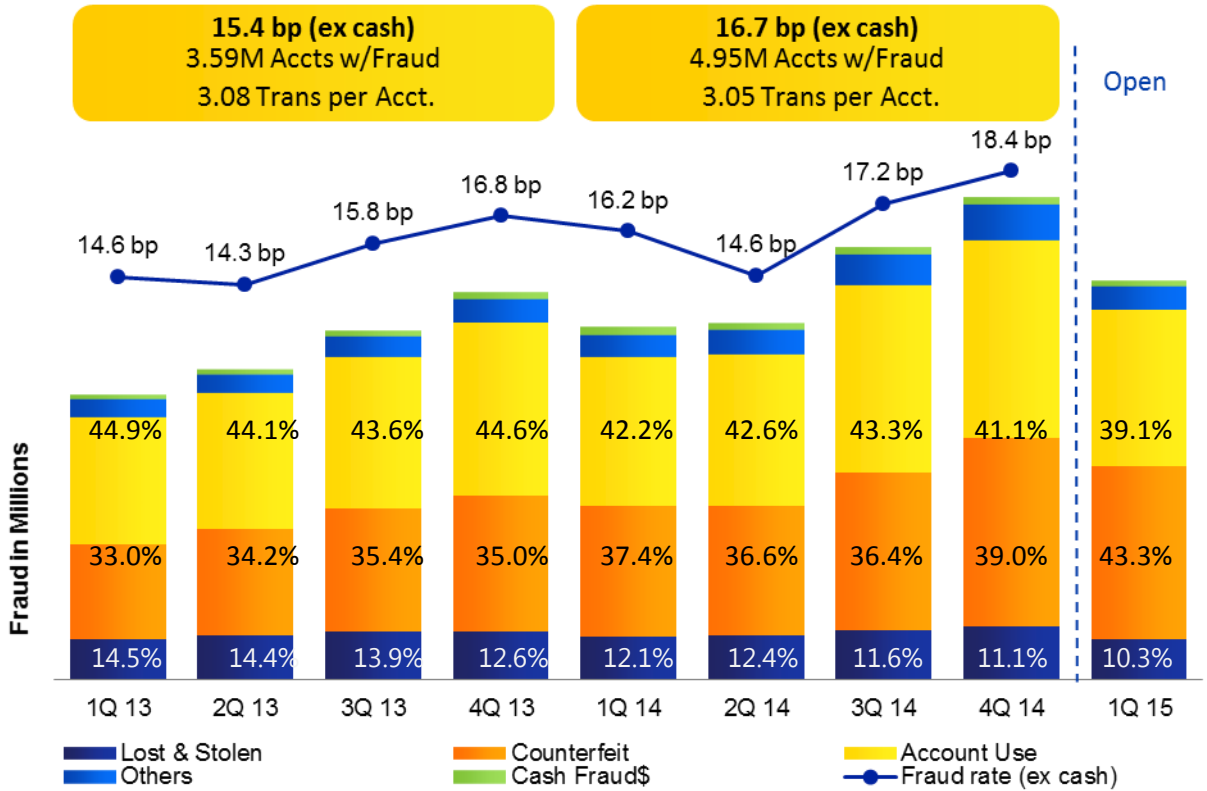
Studies, survey results, research, recommendations, and opportunity assessments are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory or other advice. Recommendations and opportunities should be independently evaluated in light of your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of any studies, survey results, research, recommendations, opportunity assessments, or other information, including errors of any kind, or any assumptions or conclusions you might draw from their use. Except where statistically significant differences are specifically noted, survey results should be considered directional only.

Agenda

- U.S. Credit Fraud Landscape
- U.S. Debit Fraud Landscape
- Measuring Fraud Efficiency
- Account Compromise Response Strategies
- EMV Risk Management Planning
- Best Practices for Managing Token Provisioning Risk
- Benefits of Accurate Fraud Advice Reporting
- Additional Resources

U.S. Credit Fraud Trends

- US fraud rates for Credit increased from 17.2 bps in 3Q 2014 to 18.4 bps in 4Q 2014, driven by a 12% increase in fraud losses.
- For Credit, counterfeit fraud experienced higher growth (20%) than Fraud Use of Account (FT6) (6%) in 4Q'14 when compared to previous quarter.
- Credit fraud accounts increased in 4Q'14 to 1.49M, as a result of a 5% increase in counterfeit fraud accounts and 18% increase in Account Use fraud accounts.



Source: TC40 client fraud reporting and Settl Sales in nominal USD (as of 04/10/2015)

U.S. Credit Top 10 Fraud MCCs

4Q ended 4Q 2014

- Grocery Stores continue to top the list of Card Present MCCs with the highest gross fraud $.
- Average ticket at AFDs is almost double the average ticket at Service Stations.
- CNP transactions are characterized by a smaller average fraud ticket size for key MCCs, primarily recurring or subscription payments.

Card Present

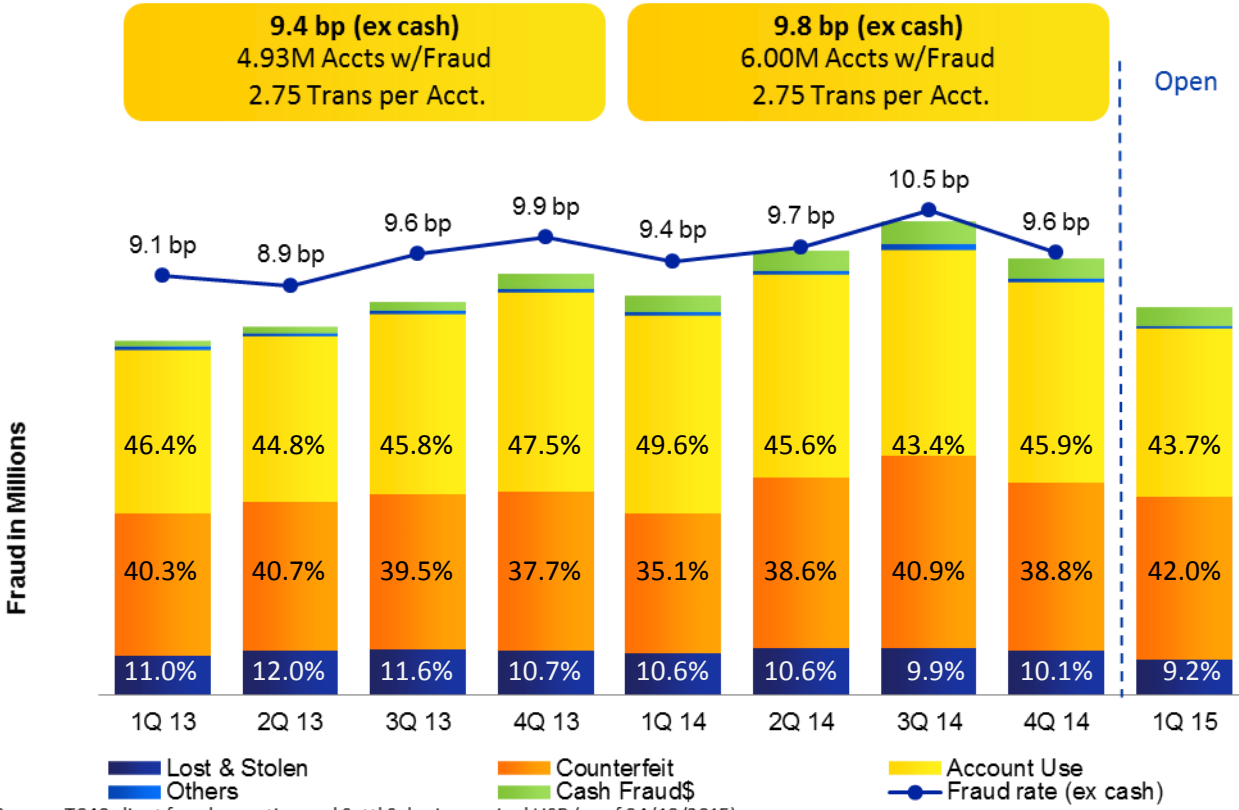
MCC DESC	MCC ID	Fraud to Settlement Ratio	Percent of Total Gross Fraud Amt	Average Fraud $ per Trans.
GROCERY STORES/SUPERMARKETS	5411	0.19%	17.42%	$144.71
DEPARTMENT STORES	5311	0.47%	6.28%	$359.11
ELECTRONICS STORES	5732	0.58%	5.59%	$882.60
AUTOMATED FUEL DISPENSERS	5542	0.10%	4.72%	$75.81
DRUG STORES & PHARMACIES	5912	0.34%	4.02%	$136.51
HOME SUPPLY WAREHOUSE STORES	5200	0.16%	3.56%	$244.00
RESTAURANTS	5812	0.05%	3.25%	$78.19
SERVICE STATIONS	5541	0.25%	2.91%	$42.88
HOTELS/MOTELS/RESORTS	7011	0.16%	2.48%	$575.01
JEWELRY STORES	5944	0.40%	2.13%	$1,518.44

Card Not Present

MCC DESC	MCC ID	Fraud to Settlement Ratio	Percent of Total Gross Fraud Amt	Average Fraud $ per Trans.
TRAVEL AGENCIES	4722	0.34%	4.69%	$446.19
ELECTRONICS STORES	5732	0.58%	4.04%	$381.40
BUSINESS SERVICES - DEFAULT	7399	0.26%	3.36%	$39.03
UNITED	3000	0.23%	3.02%	$546.67
CONTINUITY/SUBSCRIPTION MERCHT	5968	0.34%	2.59%	$32.72
MISC SPECIALTY RETAIL	5999	0.25%	2.57%	$170.97
MISC FOOD STORES - DEFAULT	5499	0.56%	2.42%	$87.43
OTHER DIRECT MARKETERS	5969	0.19%	2.30%	$161.27
TELECOMMUNICATION SERVICES	4814	0.14%	2.27%	$82.32
PROFESSIONAL SERVICES - DEF	8999	0.34%	2.26%	$160.98

U.S. Debit Fraud Trends

- US fraud rates for Debit declined from 10.5 bps in 3Q 2014 to 9.6 bps in 4Q 2014, driven by an overall 8% reduction in fraud losses.
- In 4Q 2014, the reduction in Debit was driven by counterfeit which declined by 13%. Fraud use of account (FT6) also experienced a reduction of 3%. Share of US fraud dollars was 46% for Fraud Use of Account and 39% for counterfeit in 4Q'14 for Debit products.
- Debit fraud accounts declined in 4Q'14 to 1.5M, as a result of a 11% reduction in counterfeit fraud accounts and 6% decline in Account Use fraud accounts.



Source: TC40 client fraud reporting and Settl Sales in nominal USD (as of 04/10/2015)

U.S. Debit Top 10 Fraud MCCs

4Q ended 4Q 2014

- For both Card Present and Card Not Present, average fraud ticket is lower on Debit than it is for Credit at the same MCCs.
- Subscription merchants and recurring payments are more prevalent for Debit than for Credit.
- Cash related transactions are also more prevalent for Debit – MCC 6011 in Card Present and MCC 4829 in Card Not Present.

Card Present

MCC DESC	MCC ID	Fraud to Settlement Ratio	Percent of Total Gross Fraud Amt	Average Fraud $ per Trans.
GROCERY STORES/SUPERMARKETS	5411	0.07%	15.52%	$108.77
AUTOMATED FUEL DISPENSERS	5542	0.07%	10.09%	$75.63
FINANCIAL INST/AUTO CASH	6011	0.07%	7.72%	$174.49
SERVICE STATIONS	5541	0.08%	4.33%	$39.75
RESTAURANTS	5812	0.03%	4.23%	$56.01
DRUG STORES & PHARMACIES	5912	0.11%	4.10%	$106.07
DEPARTMENT STORES	5311	0.19%	3.89%	$217.63
ELECTRONICS STORES	5732	0.35%	3.10%	$461.61
HOME SUPPLY WAREHOUSE STORES	5200	0.07%	2.95%	$164.99
DISCOUNT STORES	5310	0.12%	1.93%	$122.42

Card Not Present

MCC DESC	MCC ID	Fraud to Settlement Ratio	Percent of Total Gross Fraud Amt	Average Fraud $ per Trans.
CONTINUITY/SUBSCRIPTION MERCHT	5968	0.44%	5.68%	$35.65
MISC FOOD STORES - DEFAULT	5499	0.72%	4.40%	$67.76
TELECOMMUNICATION SERVICES	4814	0.07%	4.37%	$78.63
BUSINESS SERVICES - DEFAULT	7399	0.36%	4.22%	$18.72
CABLE, SAT, PAY TV/RADIO SVCS	4899	0.08%	3.84%	$137.50
TRAVEL AGENCIES	4722	0.39%	3.26%	$293.79
WIRE TRANSFER MONEY ORDER	4829	0.50%	2.93%	$276.55
ELECTRONICS STORES	5732	0.55%	2.90%	$207.75
INBOUND TELEMARKETING MERCHANT	5967	2.33%	2.87%	$28.99
PROFESSIONAL SERVICES - DEF	8999	0.33%	2.56%	$86.73

Measuring Fraud Efficiency

Recommend monthly and/or quarterly fraud analysis on highest fraud contributors to adjust fraud strategies.

- Portfolio segmentation (BIN, Account Range, Customer Type, Acquisition Channel, etc.)
  - Determine Risk appetite
  - False Positive Ratio analysis
- "What if" analysis for new rules, look at 13 weeks of historical data
- MCC Analysis
  - Velocity rules
  - Legitimate use average ticket vs. fraudulent average ticket
  - Average VAA score
- Fraud Type and Channel Analysis
- Fraud Forum participation for sharing information on new trends

Fraud Transaction Amount per Account × Number of Fraud Transactions per Account = Average Fraud Loss per Account × Number of Fraud Accounts = **Total Gross Fraud Losses**

Account Compromise Response Strategies

Before

(Identifying a data compromise)

- Report Common Point of Purchase (CPP) to Visa
- Analyze fraud patterns on "at risk" accounts, test fraud mitigation rules

During

(preventing fraud once a compromise is confirmed)

- Download accounts from CAMS
- Flag impacted accounts and monitor activity
- Leverage Visa Advanced Authorization (VAA) Compromised Event Reference ID (CERID)
- Align fraud controls to type of data exposed

After

(on-going, monitoring)

- Adjust fraud rules based on fraud type as fraud occurs
- Completely and accurately report fraud to Visa within 90 days of occurrence
- Consider your reissuance strategy
- Engage cardholders via educational materials or transaction alerts

EMV Risk Management Planning

Migrated Portfolio

- EMV-specific card verification values in authorization strategy
- Cardholder education
- Breach response strategy
- Card not present fraud strategies

Unmigrated Portfolio

- Set up specific fraud strategies for:
  - Accounts with expiry within 3-6 months
  - Brute force attacks
  - Account testing

Ensure the Risk function is embedded in the EMV migration project

Best Practices for Managing Token Provisioning Risk

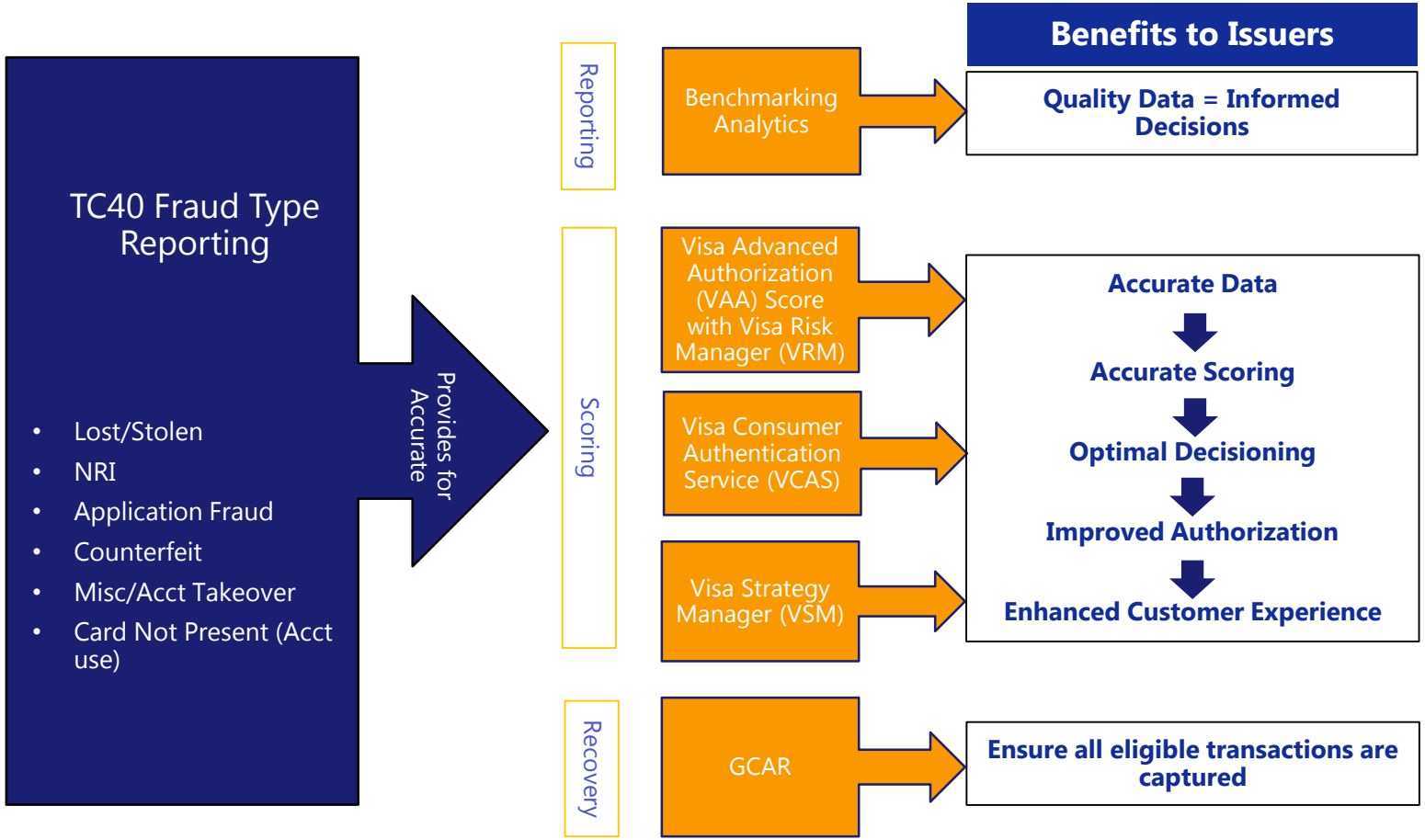
Cardholder Authentication

- Pre-provisioning Registration: Enable customers to register their mobile devices to reduce risk prior to token provisioning.
- Consumer Authentication: Verify a cardholder's address and identity using a variety of methods during the provisioning process.
- Device Authentication: Match the cardholder's mobile device location with the address on file, as well as monitor it for fraudulent activity, during the provisioning process.
- Card Authentication: Perform Card Verification Value 2 (CVV2) validation and check the card expiration date during the provisioning process.
- Visa Risk Manager (VRM): Use VRM and its suite of Web-based applications to manage token provisioning risks.
- Transaction Processing: Employ risk evaluations after token provisioning by monitoring transaction activity.

Lessons Learned

- Implementation of additional or more robust authentication strategies,
  - One time password parameters should note how recent a phone number update occurred
  - Out of wallet questions (e.g. Recurring payments)
  - When using Address Verification Services, ensure address data is uniform, accurate and up to date
  - Provide as close to real time confirmation of enrollment as possible
  - Pair as many data points available to the device and the cardholder account
    - For example – If a provisioning request is made for a phone with a card previously loaded and the zip codes do not match, this could be a red flag for a fraudulent provisioning request.
- The use of rules for newly provisioned yellow path or suspicious tokens as well as transaction monitoring can help mitigate risk
- Report fraud as a result of weak Token Provisioning process as Fraud Type 5 - Misc./Account Take Over

Benefits of Accurate Fraud Reporting



Additional Resources

Visa Business News Articles

1. Reminder: Report Fraud Activity Promptly and Accurately, June 2014
2. Assess and Optimize Fraud and Approval Performance, July 2014
3. Mitigating Fraud Risk Through Card Data Verification, September 2014
4. Updated Fraud Reporting Guidance, February 2015
5. Visa Token Provisioning Best Practices Published, April 2015

Visa Online

1. Issuer Fraud Control Manual
2. Account Data Compromise Best Practices for Issuers
3. Fraud Reporting System User's Guide

Thank you