Controlling Debit Fraud Losses

Carolina Gallegos
Director, North America Risk Services
Visa Inc.

June 16, 2014

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.

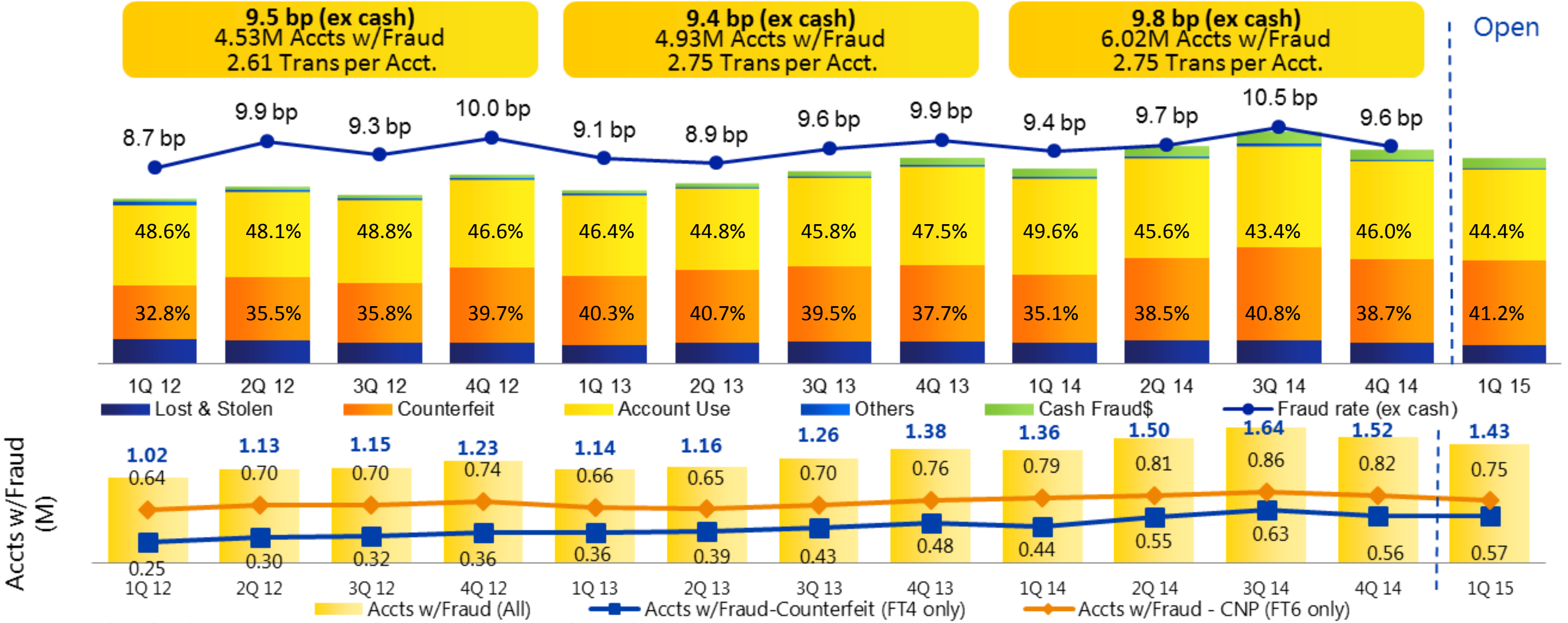
Studies, survey results, research, recommendations, and opportunity assessments are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory or other advice. Recommendations and opportunities should be independently evaluated in light of your specific business 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. Debit Fraud Trends
- Top 10 MCCs by Gross Fraud Amount
- Account Lifecycle Controls
- Fraud Schemes and Best Practices
  - ATM fraud
  - Fraudulent credits
- Additional Resources

U.S. Debit Fraud Trends

- U.S. fraud rates for Debit declined from 10.5 bps in 3Q 2014 to 9.6 bps in 4Q 2014, driven by an overall 7% reduction in fraud losses.
- In 4Q 2014, the reduction in Debit was driven by counterfeit which declined by 12%. Card-not-present (FT6) also experienced a reduction of 2%. Share of U.S. fraud dollars was 46% for CNP and 39% for counterfeit in 4Q 2014 for Debit products.
- Debit fraud accounts declined in 4Q 2014 to 1.5M, as a result of a 11% reduction in counterfeit fraud accounts and 5% decline in CNP fraud accounts.



Source: Fraud Reporting System (TC40) and VisaNet Settlement Data; Issuers have 90 days to report fraud in the "Open" quarter

Top 10 Fraud MCCs

Fraud with purchase date of 2014

Card Present

MCC		Fraud to Settlement Ratio	% of Total Gross Fraud $	Avg. Fraud Amount per Trans.
GROCERY STORES/SUPERMARKETS	5411	0.07%	15.52%	$108.77
AUTOMATED FUEL DISPENSERS	5542	0.07%	10.08%	$75.61
FINANCIAL INST/AUTO CASH	6011	0.07%	7.73%	$174.49
SERVICE STATIONS	5541	0.08%	4.33%	$39.75
RESTAURANTS	5812	0.03%	4.23%	$55.99
DRUG STORES & PHARMACIES	5912	0.11%	4.10%	$106.05
DEPARTMENT STORES	5311	0.19%	3.88%	$217.61
ELECTRONICS STORES	5732	0.35%	3.10%	$461.71
HOME SUPPLY WAREHOUSE STORES	5200	0.07%	2.95%	$164.98
DISCOUNT STORES	5310	0.12%	1.93%	$122.40

- These MCCs account for over 50% of Card Present gross debit fraud $ in the U.S.
- Highest average fraud ticket at Electronics Stores and Department Stores

Card Not Present

MCC		Fraud to Settlement Ratio	% of Total Gross Fraud $	Avg. Fraud Amount per Trans.
CONTINUITY/SUBSCRIPTION MERCH	5968	0.44%	5.69%	$35.55
MISC FOOD STORES - DEFAULT	5499	0.72%	4.39%	$67.75
TELECOMMUNICATION SERVICES	4814	0.07%	4.38%	$78.54
BUSINESS SERVICES - DEFAULT	7399	0.36%	4.22%	$18.70
CABLE, SAT, PAY TV/RADIO SVCS	4899	0.08%	3.84%	$137.12
TRAVEL AGENCIES	4722	0.39%	3.26%	$293.69
WIRE TRANSFER MONEY ORDER	4829	0.50%	2.93%	$276.51
ELECTRONICS STORES	5732	0.55%	2.90%	$207.39
INBOUND TELEMARKETING MERCH	5967	2.34%	2.88%	$28.99
PROFESSIONAL SERVICES – DEF	8999	0.33%	2.56%	$86.63

- These MCCs account for approximately 37% of Card Not Present gross debit fraud $ in the U.S.
- High occurrence of fraud at recurring and subscription merchants

Source: Fraud Reporting System (TC40) and VisaNet Settlement Data; Issuers have 90 days to report fraud in the "Open" quarter

Controls Throughout the Account Lifecycle

Screen, Monitor, Track, Adjust

New Account Set Up

- Establish authentication controls for customer account activity and updates
- Customer risk profile drives account minimums and limits
- Opt in for mobile alerts, if available

Account Monitoring

- Apply new account screening processes to requests for new or additional debit cards or PIN changes
- Review recent account activity for potential signs of account takeover

Authorization Monitoring

- Leverage VAA score
- Velocity controls
- Establish controls based on at risk data as a result of a breach
- Engage cardholder via Transaction Alerts

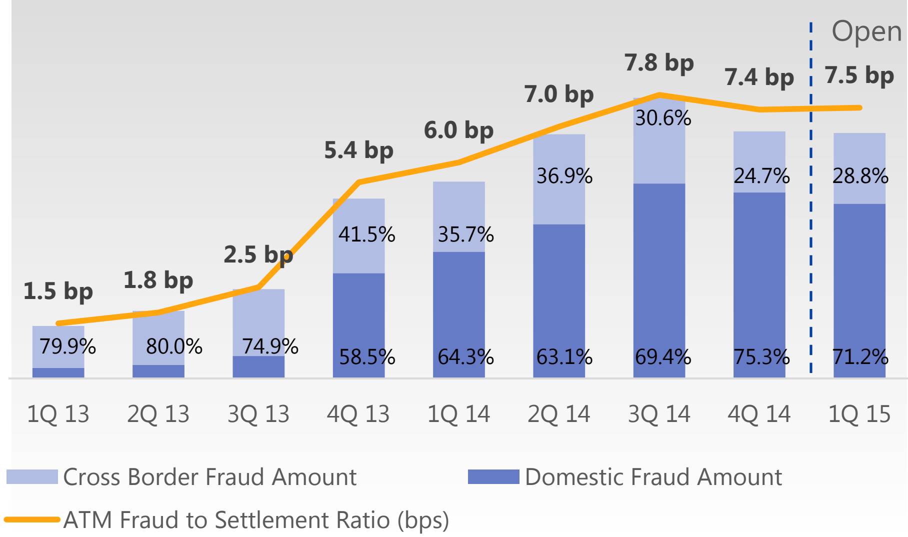
Loss Control & Reporting

- Understand root cause of fraud losses
- Make screening and monitoring process adjustments as needed
- Review the need to train / educate other divisions or cardholders on common fraud schemes

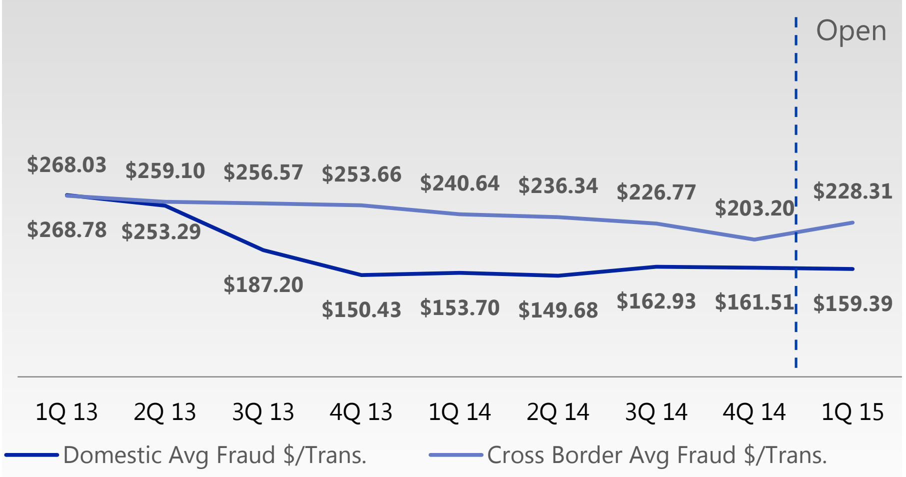
U.S. ATM Debit Fraud Trends

MCC 6011

Gross Fraud Losses by Quarter



Average Fraud Ticket by Quarter



- U.S. Debit gross fraud losses at ATMs increased by 37% from 4Q 2013 to 4Q 2014.
- Cross border represents only 17% of ATM Debit sales on U.S. issued cards, but 32% of ATM Debit fraud for 2014.

- While overall gross fraud losses have increased, the average fraud $ per transaction has been declining
- Cross border average fraud tickets remain higher than domestic, with a spike in the open quarter

Source: Fraud Reporting System (TC40) and VisaNet Settlement Data; Issuers have 90 days to report fraud in the “Open” quarter

Best Practices for ATM and PIN Management

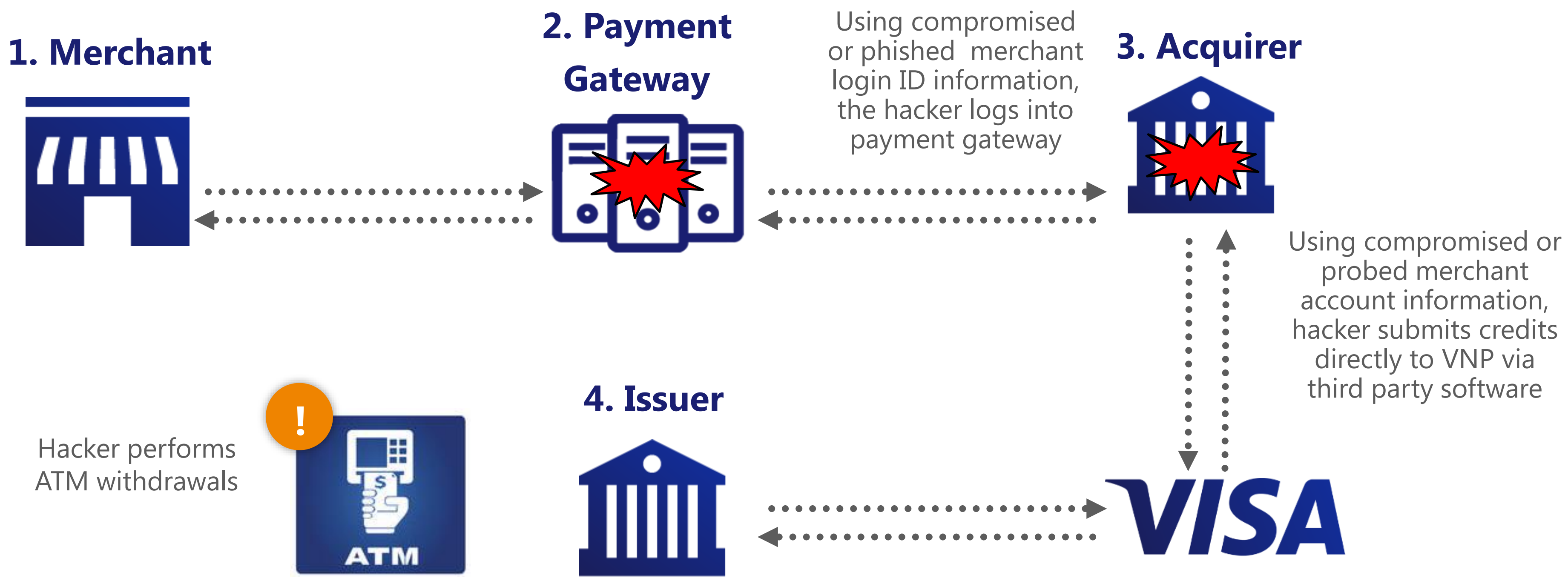
1. Be vigilant with customer authentication and PIN change practices
   - Issuers should conduct step-up authentication or additional due diligence
     - On at-risk accounts
     - After recent account changes
   - Do not use card data to authenticate customer identity
   - Continue to educate customers on fraud prevention, including
     - The importance of selecting a non-obvious PIN known only by the owners of the account
     - The perils of phishing and other common scams
2. ATM operators should check machines at least daily for any evidence of tampering



3. Issuers should utilize advanced analytics and strategies to proactively identify potential fraud patterns

Fraudulent Credits – Attack Process Flow

A simulated refund (TC06) issued by criminals posing as merchants to post funds to card accounts they've previously set up with the intention of then withdrawing the funds



How Issuers Can Mitigate Financial Losses

- Monitor cardholders’ credit, debit and prepaid card accounts for unusual credits without a previous matching debit transaction
  - Take appropriate measures to hold funds if there is suspicion of a fraudulent transaction
- Investigate any discrepancies promptly, before funds are moved into the cardholder account and subsequently released or withdrawn.
- Issuers that successfully withhold a fraudulent credit or are able to recover funds after they have been withdrawn must refund the money to acquirers via a TC 26 credit reversal.

Additional Resources

VISA

Visa Online Resources

- VBN: Visa Alerts Members to Actively Prevent Fraudulent Credits – December 19, 2013
- VBN: Updated Tips for Preventing and Mitigating ATM Cash-Out Fraud – February 20, 2014
- VBN: Updated Fraud Reporting Guidance – October 15, 2014

Public Resources for Cardholders

- Protection at the ATM, from visa.com
- Visa Security Sense

Thank You