Guideline Prevention Gift Card Fraud

Gift card fraud poses a potential threat not only to individual businesses but also to the financial integrity and reputation of our industry. To address this, the three European associations—BVCNL, GVCA, and PVD—have come together to compile an inventory of potential measures aimed at preventing or mitigating fraud-related risks. This initiative also seeks to raise awareness and encourage best practices, helping to elevate industry standards across the board.

This overview serves as a practical resource for market participants, enabling them to assess and adopt the most relevant measures for their specific circumstances. By doing so, businesses can better safeguard their operations while contributing to the overall integrity of the market.

By implementing these measures, we aim to enhance awareness within the industry and promote a higher standard of financial integrity, ensuring a safer environment for all market players.

Please note that

- This list offers a variety of potential actions but is not exhaustive.
- It does not claim to cover every risk, as fraud tactics continuously evolve.
- As a result, the overview will be periodically updated to reflect new developments and emerging threats.

Contents

Shop/Brick and Mortar Retail

	Measure
Package tempering/ Copying or photographing card numbers	1. Adjust packaging so that card number is not legible. This can be done by sticking a strip over the card number which should be removed during activation of the gift card. Merely displaying the barcode and not the card number is not effective. 2. Convert to secured packaging where both card number and activation barcode are behind a security strip or within the packaging. 3. Keep dummy cards on the shelf in shop and the inactive gift cards behind the counter. 4. Incorporate unique authenticity feature in scratch layer. 5. Use signage on gift card fixtures to alert customers to potential scam activity.
Till restrictions	1. Set business rule 'maximum balance' (e.g. max €/£150 per card). 2. Set merchant limit. This ensures that a merchant can sell a limited amount of gift cards per unit of time. 3. If self-scanning is present; set maximum amount per transaction for an activation and redemption of gift card. 4. Mandatory security code check when redeeming offline 5. Prevent activation at checkout before payment has taken place so that 'forgotten wallet' does not lead to activated gift cards (post tender activation). 6. Add a systemic block to any cards which are balance checked before activation. This is a clear indicator that cards have been tampered with and a feature which most processors offer. 7. Add geolocation technology to card distribution. Systemically block cards which are attempted to be activated in a different location to the one they should be in. This is a clear indicator that cards have been removed from one store, tampered with, and put back into a different store to avoid detection by security. 8. Use prompts on the till to alert customers to potential scams. 9. Prevent the purchase of a Gift Card with another Gift card.

Incentive/B2B sales

	Measure
Customer	1. Do not offer payment method 'payment post ordering', unless a KYB/KYC and financial credit investigation has been completed. 2. Delayed activation (i.e. 24 hours) if permitted (access to e-money should be immediate under the EMD). 3. Set credit limit at customer level. 4. When 'reshipping' ensure that old products have been removed from the market / or values are blocked.
Processor	1. Blocked sending of gift cards. 2. Send activation code to the customer via another channel (card digitally / code by mail). 3. Multi layer authentication, e.g the URL does not instantly load the gift card without further steps to verify the user then activate the gift card and load it on a separate page (this can be done in seconds with minimal impact to UX). 4. Transaction frequency – tracking in order to detect suspicious patterns or spikes in activity beyond agreed thresholds. 5. Provide easy access to all transaction info to the buyer, allowing them to extract and report details when any suspicious activity occurs, e.g if a card needs to be raised to a retailer to be blocked. 6. Provide API or in-system access to cancel codes where individual retailer API allows it. 7. Integrate with external fraud systems - e.g Stripe or Shopify for payment processing - this allows the application of additional fraud rules. These platforms use a larger database of fraud patterns across industries to detect suspicious activity. 8. Ensure there are agreed Fraud reaction processes in place between buyers, processors and retailers so that there is a seamless and fast acting process when issues do arise. 9. Use of AI and machine learning for fraud detection - integrate AI driven fraud detection systems that analyse transactions, user behaviour and use adaptive security measures to mitigate fraud risks.
System user	1. Assign correct authorisations 2. Periodically check audit trail for downloads, credit limit changes, resend e-gifts, etc. 3. Deliver bulk files via external download link/sftp

Online

	Measure
Balance check	1. Implement Re-Captcha. 2. Make security code mandatory. 3. Delay responses on repeated balance checks 4. Block IP addresses / accounts (temporarily) on repeated balance checks. 5. Block inactive cards on repeated balance checks (business rule via Service Provider). 6. Use of general error messages instead of too detailed information. 7. Maximum number of balance checks per time block (e.g. per hour). 8. Reminder users to check a website is 'https' and not a spoof site.
Activation and redemption	1. Implement re-captcha 2. Make security code mandatory 3. Limit number of gift cards (or amount) per order 4. Set up order monitoring
Accounts (customer)	1. Restrictions on amount to be spent via gift card for new accounts (accounts without an order e.g. first allow max €/£150 redemption). 2. Preventing fake accounts/shortened KYC. 3. Monitoring orders excessive use (e.g. average gift card transaction is €/£30, anything over €/£x manual review). 4. Outsource transaction monitoring to specialist (e.g. Shopify or PSP fraud module). 5. Block email and/or IP address in case of proven fraud. 6. Delivery via a facility that is password protected and/ has multi-factor authentication rather than PDF/URL.
Terms and Conditions	1. Don't allow for cashback on order cancellation or returned gift cards. 2. Prohibit resale or auctioning on unauthorised platforms. 3. Reserve the right to suspend or cancel gift cards for suspicious activity. 4. Specify geolocation restrictions for card activation and redemption. 5. Clarify loss and theft policies and conditions for replacement. 6. Define governing law and jurisdiction for disputes. 7. Prohibit use of gift cards for financial crimes like money laundering.

Training

	Measure
It's best practice to conduct mandatory training, applicable for all employees to cover essential compliance topics focusing on the practical aspects of legal, ethical, and operational compliance in a gift card environment.	Module: Anti-Fraud Practices 1. Recognizing suspicious transactions or behaviour related (i.e. instore sales, B2B orders etc.) 2. Procedures for reporting suspected fraud
	Module: Data Privacy (GDPR) 1. How to protect customer information (e.g., names, payment details) 2. Importance of confidentiality when handling personal data
	Module: Understanding AML regulations 1. Recognising red flags for money laundering (e.g., large, untraceable cash transactions). 2. Gift card misuse and how it can relate to money laundering schemes.
	Module: Bribery and Corruption 1. Definitions and examples of bribery (e.g., accepting gifts or favors in exchange for better service). 2. Avoiding Conflicts of Interest identifying and disclosing conflicts of interest (e.g., personal relationships with vendors or customers).
	Module: Handling Financial Transactions, Cash Handling and Fraud Prevention 1. Proper procedures for cash handling to avoid mistakes or fraud. 2. How to identify counterfeit currency. 3. Avoiding chargebacks and handling customer disputes.
	Module: Reporting 1. How to Report Non-Compliance 2. Ensuring whistleblower protection for employees who report misconduct.
	Module: Keeping Customers Safe 1. How to recognise and support a vulnerable customer who is being scammed. 2. How to recognise a tampered gift card. 3. How to prioritise and help a B2B buyer reporting fraudulent activity.

Sector Actions

Best Practice Guidelines	1. Work collaboratively across the sector to develop, deliver and follow best practice guidelines, such as these.
Monitoring Fraud	1. Working collaboratively with the sector and wider specialist organisations to monitor social media platforms and dark web forums where fraudsters might sell stolen gift cards or share information on exploiting vulnerabilities. 2. Share new fraudulent activity with sector colleagues and trade associations
Collaboration & Data Sharing	1. Create collaborative partnerships with external fraud prevention organizations, such as law enforcement. 2. Share non-sensitive data on fraud trends across the industry. 3. Create a shared repository of known fraudulent tactics, similar to the anonymous reporting platform, but focused on updating emerging threat patterns.

BVCNL is the Dutch industry organisation representing the interests of the gift card industry. It represents the Key Players in a €1.9 billion gift card market. With over 45 members including retailers, issuers and service providers BVCNL provides a platform and infrastructure for members to collaborate, share best practice and keep up to date with a fast growing and dynamic industry. BVCNL actively promotes the collective interests of its members. It monitors the reputation of the industry and liaises with stakeholders to create maximum benefits opportunities for its members.

The BVCNL offers its members a dedicated and anonymous platform to report instances of attempted fraud. By doing so, members can contribute to a collective effort to better understand and address emerging fraud tactics without revealing their identity. Detailed information from these reports will only be shared with other members after obtaining the explicit consent of the reporting party. This ensures a balance between privacy and collaboration, allowing the industry to learn from each other's experiences, enhance awareness, and strengthen fraud prevention measures across the industry.

BVCNL: info@bvcnl.nl

The Gift Card & Voucher Association (GCVA) is the trade body and membership organisation for gift cards and vouchers. The association represents the key players in the industry and promotes best practice for the benefit of gift card issuers, services and consumers. The GCVA's role is to protect and promote the gift card sector: keeping members up-to-date with trends, issues, challenges and opportunities; advocating on key legislation and regulation; creating opportunities for business development; commissioning relevant research; collaborating with stakeholders; delivering networking & events; and promoting the high-quality businesses that join GCVA.

GCVA has a fraud & integrity working group, as well as running quarterly Fraud Forums for our members, wherein members hear from experts in the fraud space, as well as sharing with each latest incidents and mitigation best practice. GCVA is developing relationship with law enforcement across the UK and wider Europe to better fight and deter fraudsters.

GCVA: info@gcva.co.uk

Founded in 2011, Prepaid Verband Deutschland (PVD) e. V. is an industry association representing the interests of the prepaid industry operating in Germany. These include, for example, Content and payment providers, issuers, distributors, sales and acceptance partners as well as incentive and reward agencies.
By actively developing the prepaid market, the association represents the interests of its members and is the point of contact for politicians, authorities and the public. Further the PVD organizes the Prepaid Congress, which takes place annually in Berlin.
At present about 30 companies are members of the PVD.

PVD: info@prepaidverband.de

Version: November 2024