

ASC X9 TR 48–2018

Card-Not-Present (CNP) Fraud Mitigation in the United States:

Strategies for Preventing, Detecting, and Responding to a Growing Threat



A Technical Report prepared by:
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Registered with American National Standards Institute

Date Registered: June 3, 2018

American National Standards, Technical Reports and Guides developed through the Accredited Standards Committee X9, Inc., are copyrighted. Copying these documents for personal or commercial use outside X9 membership agreements is prohibited without express written permission of the Accredited Standards Committee X9, Inc. For additional information please contact ASC X9, Inc., 275 West Street, Suite 107, Annapolis, Maryland 21401.

Table of Contents

1	Purpose, Scope, and Stakeholders	1
1.1	Primary stakeholders	2
1.1.1	Issuer	2
1.1.2	Issuer processor	2
1.1.3	Merchant	2
1.1.4	Acquirer, processor, and payment gateway	2
1.1.5	Payment card network	3
1.1.6	PIN debit network	3
1.2	CNP Transaction Scenarios	3
1.2.1	E-commerce	3
1.2.2	Mobile commerce	4
1.2.3	Mail or telephone order (MOTO)	5
1.2.4	Order online and pickup in-store	6
2	Normative References	6
3	Terms and Definitions	7
4	Symbols and Abbreviated Terms	16
5	Protect Against Data Theft	17
5.1	Identify sensitive data and apply incremental controls to protect it	18
5.2	Reduce the value of sensitive data at rest and in transit	18
5.2.1	Encryption	19
5.2.2	Tokenization	20
5.3	Identify and secure the systems, networks, and facilities used to process sensitive data	20
5.3.1	Document all hardware, software, transmissions, and connections	21
5.3.2	Apply enhanced physical and logical security controls for payment processing technology	21
5.3.3	Implement vulnerability management and malware detection controls	22
5.3.4	Log and monitor payment system activity	22
5.3.5	Test payment security system controls regularly to identify and address vulnerabilities	23
5.3.6	Restrict access to systems and facilities used to process or store sensitive payment information	24
5.4	Identify roles with access to sensitive data and apply incremental human resource controls	24
5.5	Manage third party service provider, processor, and vendor risk	25
5.6	Demonstrate senior management commitment, leadership, and accountability	26
6	Landscape of Card-Not-Present (CNP) Fraud Attacks	26
6.1	CNP Attacks to Steal Data	26
6.1.1	Malware and spyware attacks	26
6.1.2	Botnet and scripted attacks	28
6.1.3	Identity testing or velocity attacks	30
6.1.4	Spoofing attacks	31
6.1.5	Triangulation fraud attacks	32
6.2	CNP Attacks to Attempt Fraud	32
6.2.1	Account takeover attacks	32
6.2.2	New account or application fraud attack	34
6.2.3	Call center fraud attacks	35

ASC X9 TR 48–2018

7	Detect and Prevent CNP Fraud: Stakeholder Mitigation Tools and Approaches	37
7.1	Merchant CNP fraud mitigation tools and approaches	37
7.1.1	Authentication	37
7.1.2	Merchant order management systems to detect fraudulent transactions	41
7.1.3	Merchant transaction monitoring and customer validation services	41
7.1.4	Merchant manual review fraud prevention	43
7.1.5	Order online and pick-up merchandise in store	45
7.1.6	Mail or telephone order (MOTO)	46
7.1.7	Merchant summary recommendations	47
7.2	Merchant acquirer and payment gateway CNP fraud tools for merchants	47
7.2.1	Merchant acquirer	48
7.2.2	Payment Gateway	49
7.3	Issuer and issuer processor CNP fraud mitigation tools and approaches	49
7.3.1	Payment transaction authentication analytics	50
7.3.2	Payment card authentication	51
7.3.3	Payment transaction fraud risk analysis	52
7.3.4	Post transaction analysis	55
7.4	Payment card network CNP fraud mitigation tools and approaches	55
7.4.1	Payment card network authentication	56
7.4.2	Transaction Authentication	57
7.4.3	Security: Second layer defense systems	60
8	Respond: Implement an Adaptive CNP Fraud Mitigation Model	60
8.1	Identify, measure, and track key metrics and trends	60
8.1.1	Merchants	61
8.1.2	Issuers	61
8.2	Establish a fraud feedback loop through post-transaction analysis	62
8.3	Monitor industry trends	62
8.3.1	Merchants	62
8.3.2	Issuers	62
8.4	Perform an annual assessment and update of strategies, policies, and practices	62
8.4.1	Review and adjust the CNP fraud mitigation plan and models	63
8.4.2	Review and update the payment information security plan	63
8.4.3	Verify third party service providers and vendors are meeting security requirements	63
	Annex A - Card-not-Present (CNP) Transaction Flow Steps	64
	Annex B - Stakeholder CNP Fraud Mitigation Self-Assessment Checklists	69
	Annex C – CNP Consumer Authentication Methods, Tools and Approaches	78
	Annex D - 3DS 1.0 versus EMV 3DS Comparison	87
	Annex E – CNP Attacks and Tools Matrix	88
	Annex F – Bibliography	89

Foreword

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Committee X9, Incorporated, 275 West Street, Suite 107, Annapolis, MD 21401. This document is registered as a Technical Report according to the "Procedures for the Registration of Technical Reports with ANSI." This document is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to: Attn: Executive Director, Accredited Standards Committee X9, Inc., 275 West Street, Suite 107, Annapolis, MD 21401.

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online <http://www.x9.org>

Copyright © 2018 ASC X9, Inc.
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of the publisher. Published in the United States of America.

ASC X9 TR 48–2018

Introduction

This Technical Report is a product of the Accredited Standards Committee X9 Financial Industry Standards, and was generated by the X9A 23 CNP Fraud Mitigation group in the U.S.

This document summarizes guidelines to mitigate CNP fraud in the U.S. It identifies the primary types of CNP fraud attack trends currently impacting the payments industry and outlines the types of CNP fraud mitigation tools and strategies employed by industry stakeholders, such as merchants, acquirers, processors, payment gateways, issuers, and payment card networks. The document also provides information and recommendations for industry stakeholders to evaluate their approaches to mitigating CNP fraud and to reducing overall fraud losses.

The goal of this Technical Report is to provide legitimate CNP industry stakeholders with information to better understand the risks presented by criminal activity to more effectively prevent, detect, and manage fraud. Industry stakeholders should be aware of their potential vulnerabilities to CNP fraud, as well as the tactics and tools to deter, detect, and respond to fraud attacks. No stakeholder is without risk as criminals work continuously to develop new and improved attack vectors and tools.

Not every fraud prevention tool is suitable for every stakeholder. Stakeholders should make their own independent decisions about anti-fraud tools that represent the optimal balance between effectiveness versus the cost, commercial impact, operational complexity, and time necessary to implement. This Technical Report aims to help stakeholders make those decisions.

Suggestions for the improvement or revision of this Technical Report are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 107, Annapolis, MD 21401 USA.

This Technical Report was processed and registered for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Technical Report does not necessarily imply that all the committee members voted for its approval.

At the time this Technical Report was published, the X9 committee had the following members:

Roy C. DeCicco, X9 Chairman
Angela Henderscott, X9 Vice Chair
Steve Stevens, Executive Director
Janet Busch, Program Director

Organization Represented

Representative

ACI Worldwide	Doug Grote
American Bankers Association	Diane Poole
American Express Company	David Moore
Bank of America.....	Daniel Welch
Bank of New York Mellon	Arthur Sutton
Blackhawk Network.....	Anthony Redondo
Bloomberg LP	Corby Dear
Capital One	Marie LaQuerre
Citigroup, Inc.	Karla McKenna
CLS Bank.....	Ram Komarraju
Conexus, Inc.	Gray Taylor
CUSIP Service Bureau	Gerard Faulkner

Delap LLP	Andrea Beatty
Delap LLP	Darlene Kargel
Deluxe Corporation.....	Angela Hendershott
Diebold Nixdorf	Bruce Chapa
Discover Financial Services	Michelle Zhang
Dover Fueling Solutions	Steven Bowles
Dover Fueling Solutions	Bradford Loewy
eCurrency	David Wen
Federal Reserve Bank.....	Mary Hughes
First Data Corporation	Lisa Curry
FIS	Stephen Gibson-Saxty
Fiserv	Dan Otten
FIX Protocol Ltd - FPL.....	Jim Northey
Futurex.....	Ryan Smith
Gilbarco	Bruce Welch
Harland Clarke.....	John McCleary
IBM Corporation	Todd Arnold
Ingenico	Rob Martin
ISARA Corporation	Alexander Truskovsky
ISITC.....	Lisa Iagatta
ITS, Inc. (SHAZAM Networks).....	Manish Nathwani
J.P. Morgan Chase.....	Roy DeCicco
KPMG LLP.....	Mark Lundin
MagTek, Inc.....	Mimi Hart
MasterCard Europe Sprl.....	Mark Kamers
NACHA The Electronic Payments Association	Priscilla Holland
National Security Agency	Paul Timmel
Nautilus Hyosung	Joe Militello
NCR Corporation	David Norris
Office of Financial Research, U.S. Treasury Department	Thomas Brown Jr.
PCI Security Standards Council	Troy Leach
RouteOne	Chris Irving
RouteOne	Jenna Wolfe
SWIFT/Pan Americas.....	Karin DeRidder
SWIFT/Pan Americas.....	Frank Vandriessche
Symcor Inc.....	Debbi Fitzpatrick
TECSEC Incorporated.....	Ed Scheidt
The Clearing House.....	Sharon Jablon
U.S. Bank.....	John King
U.S. Commodity Futures Trading Commission (CFTC).....	Robert Stowsky
USDA Food and Nutrition Service	Kathy Ottobre
Vantiv LLC	John Hall
VeriFone, Inc.	Dave Faoro
VISA.....	Kim Wagner
Wells Fargo Bank	Mark Schaffer

At the time this Technical Report was published, the X9A Retail Payments subcommittee had the following members:

Guy Berg, Chairman

Organization Represented

Representative

Bank of America	Cathy Tuntland
Bank of America	Daniel Welch

ASC X9 TR 48–2018

Bank of America.....	Terri Willis
CDP, Inc.....	Johnny Sena
Conexus, Inc.	Alan Thiemann
Conexus, Inc.	Linda Toth
Diebold Nixdorf	Bruce Chapa
Discover Financial Services.....	Michelle Zhang
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Marianne Crowe
Federal Reserve Bank	Mary Hughes
Federal Reserve Bank	Heather Hultquist
Federal Reserve Bank	Janet LaFrence
Federal Reserve Bank	Angela Lawson
Federal Reserve Bank	David Lott
Federal Reserve Bank	Patti Ritter
First Data Corporation.....	Simone Arnold
First Data Corporation.....	Annamarie Corrigan
First Data Corporation.....	Guy Glauser
Fiserv	Allen Heimerdinger
Fiserv	Dan Otten
J.P. Morgan Chase	Clinton Jones
Mark Tiggas	Mark Tiggas
MasterCard Europe Sprl	Carl Jansson
Navy Federal Credit Union	Michael Deegan
Navy Federal Credit Union	April Haynes
Navy Federal Credit Union	Vicki Shapiro
Navy Federal Credit Union	Tynika Wilson
NCR Corporation	Jackie Farone
NCR Corporation	Rick Fender
NCR Corporation	Stephen Gawne
NCR Corporation	Gregg Simmons
PCI Security Standards Council	Ralph Poore
SWIFT/Pan Americas	Karin DeRidder
Symcor Inc.	Debbi Fitzpatrick
Texas DSHS WIC EBT	Duane Grabarschick
Texas DSHS WIC EBT	John Hannemann
USDA Food and Nutrition Service	Lisa Gifaldi
USDA Food and Nutrition Service	Patrick Kelley
USDA Food and Nutrition Service	Erin McBride
USDA Food and Nutrition Service	Kathy Ottobre
VeriFone, Inc.....	Brad McGuinness
Viewpointe	Richard Luchak
Wayne Fueling Systems	Bradford Loewy
Wells Fargo Bank.....	Sotos Barkas
Wells Fargo Bank.....	Andrew Garner
Wells Fargo Bank.....	Phillip Griffin
Wells Fargo Bank.....	Jeff Harmon
Wells Fargo Bank.....	Mark Schaffer
Wyoming Department of Health WIC Program.....	Tina Fearneyhough
Wyoming Department of Health WIC Program.....	Melissa Sosa
Wyoming Department of Health WIC Program.....	David Spindler

Under ASC X9, Inc. procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or technical report(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or technical report.

At the time this Technical Report was approved, the X9 X9A23 CNP Fraud Mitigation group which developed this technical report had the following active members:

Guy Berg, Chairman; Janet LaFrence, Vice Chair; and Susan Pandy, Project Editor

The following individuals and organizations contributed to the preparation of this document:

Organization Represented	Representative
Bank of America	Dan Welch
Best Buy	Adam Marzolf
Best Buy	Joe Vasterling
Conexus, Inc.	Linda Toth
Consultant	Leland Englehardt
Federal Reserve Bank of Boston	Marianne Crowe
Federal Reserve Bank of Boston	Susan Pandy
Federal Reserve Bank of Atlanta	David Lott
Federal Reserve Bank of Minneapolis	Guy Berg
Federal Reserve Bank of Minneapolis	Janet LaFrence
Merchant Advisory Group	Laura Townsend
National Institute of Standards and Technology	Paul Grassi
Nordstrom	Byran Penny
Visa	Andrew McGloin
Visa	Kevin Weller

This is a preview of "ASC X9 TR 48-2018". [Click here to purchase the full version from the ANSI store.](#)

1 Purpose, Scope, and Stakeholders

Card-not-present (CNP) fraud, the unauthorized use of a payment card for any transaction where the cardholder does not physically present the payment card, poses significant risk to today's payments ecosystem comprised of primary stakeholders such as issuers, merchants and their acquirers, processors, payment gateways, payment networks, PIN debit networks, and other relevant businesses. This Technical Report presents guidelines for the mitigation of CNP fraud for all relevant impacted industry stakeholders, such as merchants, acquirers, issuers, payment card networks, online payment service providers, payment processors, and hardware and software providers. This Technical Report addresses the environment of payment cards, such as credit, debit, and prepaid, but does not extend to private label cards, which are out of scope. Given the high cost of CNP fraud in the U.S., these guidelines are designed to help stakeholders understand the: 1) landscape of CNP fraud attacks; 2) how to protect against data theft; 3) how to detect and prevent CNP fraud using mitigation tools and processes; and 4) how to respond and implement an adaptive CNP fraud mitigation model. These guidelines are intended to provide a benchmark checklist of the CNP mitigation tools, procedures, and strategies that should be considered for effective CNP fraud mitigation.

According to the U.S. Department of Commerce, U.S. online retail sales nearly quadrupled in the decade from 2005-2015, and in 2016 accounted for \$394.9 Billion and 8.1 percent of total retail sales.¹ As of the third quarter of 2017, U.S. online retail sales accounted for 9.1 (adjusted) percent of total retail sales.² In the third quarter of 2017, U.S. mobile commerce spending was 23 percent of the total e-commerce retail sales, according to Statista.³ In the U.S., CNP fraud accounts for approximately 50 percent of total fraud losses sustained, according to various industry resources. This increase in CNP fraud can have significant consequences for small and medium businesses as well as large enterprises, requiring all companies to be prepared with the proper fraud mitigation tools and strategies.

The U.S. payments industry is preparing for a significant increase in card-not-present (CNP) attacks. With the migration from magnetic stripe (magstripe) to EMV chip cards at the point-of-sale (POS) and the anticipated shift in fraud to the CNP channel, it is important to understand how this will impact e-commerce and m-commerce. Card-not-present channels include e-commerce, m-commerce, interactive voice response (IVR) units, telephone orders, and mail orders. Consumers are also buying more goods online, using their traditional desktop computers or mobile devices and commerce is expanding across digital channels, creating more opportunities for fraud.

Although these guidelines are less restrictive than a standard, they offer suggestions on the recommended considerations to achieve enhanced security practices for adoption, as appropriate, by all relevant stakeholders within the payment card system. This Technical Report also provides information for assessors, auditors, and regulators to evaluate fraud risks and controls in the overall card payment ecosystem. Proactive implementation of these guidelines by industry stakeholders will help them to mitigate CNP fraud and reduce fraud losses within the U.S. payment card industry.

All recommendations described in this Technical Report are compatible with and supplemental to existing standards as outlined in §2 – Normative References. Certain recommendations may be outside the scope of current standards as referenced in §2 – Normative References. In addition to CNP fraud mitigation tools and a

¹ U.S. Census Bureau (2017, Feb. 17).) *Quarterly Retail E-Commerce Sales 4th Quarter 2016*. U.S. Department of Commerce. Retrieved from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

(2017, Nov. 17) *Quarterly Retail E-Commerce Sales 3rd Quarter 2017*. U.S. Department of Commerce. Retrieved from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

² U.S. Census Bureau (2017, Nov. 17) *Quarterly Retail E-Commerce Sales 3rd Quarter 2017*. U.S. Department of Commerce. Retrieved from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

³ Statista (n.d.) *M-commerce share of total digital commerce spending in the United States from 2nd quarter 2010 to 3rd quarter 2017*. Retrieved from <https://www.statista.com/statistics/252621/share-of-us-retail-e-commerce-dollars-spent-via-mobile-device/>.