

How to Use This Manual

The explosion in electronic payments in recent years has created opportunities for significant processing efficiencies, faster clearance of payments, and incentives for the development of new technologies that provide an increasing number of consumers with the option to make electronic transfers of funds. Even before the dramatic increase in electronic payments attributable to the Internet, consumers were relying on debit cards to make transfers to third parties and on automated teller machines (ATMs) to withdraw funds from or to transfer funds between financial institution accounts. A study by the Federal Reserve Board reveals that in 2000, retail electronic payments accounted for 40.5 percent of all retail noncash payments.¹ That figure has likely increased, as the forums in which such payments frequently occur, such as online auctions, electronic bill presentment and payment, and person-to-person payments, have become significantly more popular in the past few years. Moreover, the number of checks written for retail noncash payments actually declined from 49.5 billion to 42.5 billion between 1995 and 2000.² While no one is predicting that we will become a “checkless” or “paperless” payment society, it seems clear that electronic payments will increase both in number and value in the near future.

These developments promise to offer seamless transactions that provide security for sellers who wish to avoid the risks of forgery and insufficient funds associated with checks and for buyers who wish to ensure that their payments are received and processed in a timely fashion. Moreover, these developments provide significant opportunities for credit unions to reduce costs related to the processing of checks and to enter potentially profitable business areas of electronic payment.

These opportunities, however, are not without risk. While electronic payments can avoid many of the problems of fraud and forgery that are related to checks, they pose their own, somewhat uncharted, susceptibility to wrongdoing. Physical cards that are necessary to initiate electronic transactions, such as credit and debit cards, can be stolen or misused. Devices that give consumers access to accounts, such as passwords and secret codes, can be fraudulently obtained

-
1. Geoffrey R. Gerdes and Jack K. Walton, II, *The Use of Checks and Other Noncash Payment Instruments in the United States*, Federal Reserve Bulletin 360-61 (August 2002).
 2. *Id.*

and used to acquire extensions of credit or currency. Computerized transfers can be vulnerable to “hacking” or misuse by insiders at credit unions or employees of firms. Perhaps the greatest threat comes from the increasing exposure of consumers, merchants, and credit unions to “identity theft” in which imposters either use stolen credit cards and access devices to make unauthorized purchases and withdrawals or open accounts using the names and information of victims who are unaware of the fraudulent activity. Recent enactment of federal legislation, the Fair and Accurate Credit Transactions Act of 2003, recognizes that identity theft has become a major concern for consumers and, hence, for the financial institutions that maintain the accounts that identity thieves attempt to access. As discussed in this manual, that act imposes certain obligations on financial institutions that are intended to minimize the occurrence of and risks to consumers associated with identity theft.

PURPOSE OF THIS MANUAL

NAFCU's EFT Fraud Protection for Credit Unions: From Identity Theft to Wire Transfer Fraud helps credit unions understand the legal principles governing the electronic payment mechanism and provides practical guidance to help credit unions detect and deter electronic fraud. The purpose of the manual is:

- To recommend procedures that facilitate detection of fraudulent schemes that employ electronic payment systems and thus reduce a credit union's losses from electronic fraud.
- To provide credit unions with an understanding of how legal principles allocate the losses that result from electronic payment fraud.
- To provide credit unions with information about schemes that fraudulent actors frequently use to defraud credit unions and members through the use of electronic payment systems.
- To provide a convenient reference source of regulations and laws that govern electronic fraud.
- To help credit unions provide useful assistance to members who may be able to take steps to detect or deter fraud and identity theft.

ORGANIZATION OF THIS MANUAL

In each chapter of *NAFCU'S EFT Fraud Protection for Credit Unions: From Identity Theft to Wire Transfer Fraud*, we provide important procedures for credit union personnel to implement to help detect and deter fraud in their institutions. The manual is organized as follows:

Chapter 1: Introduction to Electronic Payments Fraud

This chapter provides the background to understand the risks involved in EFT transactions, the types of electronic fraud, and the law governing EFT transactions. It also explains the content of this manual.

Chapter 2: Credit Card Fraud

Chapter 2 deals with the increasing incidence of credit card fraud. It explains how credit cards work, the means that fraudulent actors use to obtain and misuse credit cards, and the law that governs the allocation of losses that result from fraud. Chapter 2 provides guidance and checklists that credit unions can both use and provide to members to deter and detect the fraudulent use of credit cards.

Chapter 3: Consumer Electronic Bill Payment and Presentment and Person-to-Person Payments

Chapter 3 introduces the loss allocation principles and means of fraud detection and deterrence that apply to various electronic transactions that consumers utilize to transfer funds to or from their credit union accounts. As a model for this discussion, this chapter discusses in-depth relevant recent consumer electronic fund transfers. These involve electronic bill payment and presentment and person-to-person payments. These transactions are governed by the legal principles set forth in the federal Electronic Fund Transfer Act and Regulation E of the Federal Reserve Board. The chapter explains how each of these devices operates, the means that fraudulent actors use to obtain and misuse credit cards, and the details of the Electronic Fund Transfer Act that determine how losses from fraud are allocated between consumers and their financial institutions. As in Chapter 2, Chapter 3 provides guidance and checklists that credit unions can both use and provide to members to deter and detect the fraudulent use of credit cards.

Chapter 4: Fraud Involving ATM and Debit Cards

Transactions involving ATM and debit cards are governed by the same legal principles that apply to electronic fund transfers for automated clearinghouse (ACH), electronic bill presentment and payment, and person-to-person payments. Thus, this chapter recaps the analysis found in Chapter 3 and applies the relevant loss allocation principles and guidance for fraud prevention to the ATM card and debit card setting. In addition, the chapter provides a discussion of the settlement of the recent litigation involving the “honor all cards” policies of MasterCard and Visa and the implications of that settlement.

Chapter 5: Wire Transfer and ACH Fraud

While Chapters 2, 3, and 4 are concerned with electronic fraud that primarily affects consumers, Chapter 5 is concerned with fraud in the transmitting of wholesale wire transfers, which primarily affects businesses. These wire transfers typically involve large sums of money and can involve transactions between financial institution accounts at significant distances. Thus, even stopping a small number of fraudulent incidents may save credit unions from incurring either large losses or large fees that would otherwise have to be expended to recover funds from accounts to which they were fraudulently directed. The chapter discusses how the creation of “security procedures” may minimize the risk of wire transfer fraud and shift the risk of those losses that ultimately materialize.

Chapter 6: Identity Theft

Each of the types of electronic fund transfer fraud discussed in this manual can involve some form of identity theft. Chapter 6 provides a general discussion of the problem of identity theft and offers a comprehensive list of recommendations for credit unions and their members to take both to avoid identity theft and to minimize the losses that may materialize once it has occurred. In addition, Chapter 6 contains a discussion and analysis of recent regulations that may reduce identity theft. These include the recent final rule promulgated by the Department of the Treasury and other federal agencies to implement Section 326 of the USA PATRIOT Act and the Fair and Accurate Credit Transactions Act of 2003. The Department of the Treasury final rule sets forth the necessary customer verification procedures that financial institutions must follow with respect to new accounts. In a separate discussion, Chapter 6 analyzes the recent interagency guidance concerning the obligations of financial institutions to ensure the security and confidentiality of sensitive customer information.

Chapter 7: The Check 21 Act and Substitute Checks

Recent federal legislation, the Check 21 Act, facilitates broader use of electronic check processing. The legislation creates a new type of negotiable instrument, called a “substitute check,” that is used by financial institutions in order to reconvert checks that have been reduced to electronic data back into their original physical form. Chapter 7 discusses how the reconversion process occurs, and explains the legal implications of creating, transferring, and receiving a substitute check.

Appendixes

For your convenience, the manual also contains regulatory reference materials, including:

- Appendix A: Relevant Provisions of Electronic Fund Transfer Act
- Appendix B: Relevant Provisions of Truth-in-Lending Act
- Appendix C: Relevant Provisions of Regulation E
- Appendix D: FTC Guidance for Lost or Stolen Cards
- Appendix E: NCUA Letters to Credit Unions 02-CU-08 Re: Account Aggregation Services
- Appendix F: Consumer Liability to Credit Union for Fraudulent Use of Consumer’s Account
- Appendix G: NCUA Letters to Credit Unions 03-CU-08 Re: Weblinking Relationships
- Appendix H: NCUA Letters to Credit Unions 02-CU-16 Re: Protection of Credit Union Internet Addresses
- Appendix I: NCUA Letters to Credit Unions 02-FCU-04 Re: Weblinking
- Appendix J: Final Rule Implementing Section 326 of the USA PATRIOT Act
- Appendix K: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

- Appendix L: SR 01-11 (SUP) Re: Identity Theft and Pretext Calling and NCUA Letters to Credit Unions 01-CU-09 Re: Identity Theft and Pretext Calling
- Appendix M: Instructions for Completing the ID Theft Affidavit
- Appendix N: UCC Article 4A
- Appendix O: NCUA Letters to Credit Unions 01-CU-10 Re: Authentication in an Electronic Banking Environment
- Appendix P: The Fair and Accurate Credit Transactions Act