Capítulo Criminológico Vol. 36, Nº 2, Abril-Junio 2008, 123 - 153
ISSN: 0798-9598

VARIABLES ASOCIADAS A LA CONSUMACIÓN Y AL AGOTAMIENTO DEL FRAUDE MEDIANTE TRANSFERENCIAS BANCARIAS POR VÍA ELECTRÓNICA

Luis Gerardo Gabaldón* y Nicanora Becerra M.**

* Profesor Titular de Derecho Penal y Criminología en las Universidades de Los Andes, Mérida; Católica Andrés Bello, y Central de Venezuela, Caracas y Profesor Invitado en el Departamento de Sociología e Investigador Titular Asociado del Instituto para la Investigación Social, Universidad de Nuevo México, Albuquerque, durante 1997. Miembro del Sistema de Promoción del Investigador, Nivel IV. Se ha desempeñado como Consultor Internacional del Ilanud, Ecuador, en 1994, de la Fundación Institucionalidad y Justicia, Inc., República Dominicana y del Forum Comunitario de Combate á Violencia, Salvador, Brasil, en 2000, de la Comunidad Andina de Naciones, en 2001 y de Nueva Sociedad en 2004 y ha sido miembro de la Comisión de Reforma Policial entre 2006 y 2007. Es autor de 11 libros y 70 artículos en materias de su especialidad. E-mail: lgabaldón@ucab.edu.ve

** Es egresada como Criminólogo y Abogada de la Universidad de Los Andes, Mérida. Actualmente es Asistente de Investigación en el proyecto sobre Fraude electrónico, lealtad empresarial y cultura corporativa, desarrollado en el Núcleo de Estudios sobre Delincuencia Económica del Centro de Investigaciones Jurídicas, Universidad Católica Andrés Bello. Se ha desempeñado como asesora en el desarrollo de trabajos de grado sobre desempeño policial, políticas criminales y características psicológicas relacionadas con conductas desviadas desde 2003.

RESUMEN

El presente artículo analiza las variables asociadas a la defraudación mediante transferencias bancarias indebidas en el periodo comprendido entre mayo de 2004 y agosto de 2006. Utilizando como marco de referencia la teoría de las oportunidades y el análisis situacional del delito, se formularon proposiciones explicativas de la defraudación considerando el valor de la oportunidad delictiva, estimado de acuerdo al monto disponible en cuentas bancarias y al perfil socioeconómico del cliente, y de la magnitud de la oportunidad delictiva, estimada de acuerdo a la disponibilidad y activación de medidas de seguridad, tiempo de ejecución y sitios donde se efectúan los retiros de los fondos transferidos. Se incorporaron al análisis características de los titulares de cuentas, como edad, sexo, nivel educativo y ocupación. Los montos disponibles en las cuentas, como indicadores de valor, se encuentran estrechamente asociados al traslado de fondos a cuentas receptoras y a la victimización múltiple. Los primeros días de la semana y el tiempo transcurrido desde la transferencia a la cuenta receptora, se encuentran significativamente asociados al agotamiento del fraude. Se recomienda incrementar los controles relativos a las alertas y la activación de procedimientos bancarios, así como expandir el conocimiento sobre el comportamiento de los titulares de las cuentas bancarias para explorar la incidencia de medidas que pudieran incidir en la protección frente al fraude.

Palabras clave: Fraude, transferencias bancarias, teorías de las oportunidades, análisis situacional del delito, oportunidad delictiva.

Recibido: 06-11-2007 • Aceptado: 07-03-2008

VARIABLES ASSOCIATED WITH THE PERPETRATION AND EXHAUSTION OF ELECTRONIC BANK TRANSFER FRAUD

ABSTRACT

This article analyzes variables related to fraud through illegitimate bank transfers in one Venezuelan bank between May, 2004 and August, 2006. Using the theory of opportunities and situational crime analysis as a referential framework, proposals explaining fraud were formulated considering the value of the criminal opportunity, estimated according to the amount available in bank accounts and the socio-economic profile of the client, and the magnitude of the criminal opportunity, estimated according to the availability and activation of security measures, time for execution and sites where transferred funds are withdrawn. Account owner characteristics were also analyzed, noting sex, age, education and occupation. The amounts available in the accounts, as value indicators, are closely associated with fund transfer to receiving accounts and multiple victimization. The early days in a week and the time lapsed since transfer to the receiving account are associated significantly with stopping fraud. Recommendations are to increase controls related to alerts and bank procedure activation, as well as increasing knowledge about bank account owner behaviour in order to explore the effect of measures that could afford protection against fraud.

Key wods: Fraud, bank transfers, opportunities theory, situational crime analysis, criminal opportunity.

1. TECNOLOGÍAS DE LA INFORMACIÓN, BANCA VIRTUAL Y FRAUDE ELECTRÓNICO

Las Tecnologías de la Información podrían entenderse como la integración y convergencia de la informática, las telecomunicaciones y la técnica para el procesamiento de datos, donde sus principales componentes

son el factor humano, los contenidos de la información, el equipamiento, el software y los mecanismos de intercambio electrónico de información, los elementos de política y regulación, y los recursos financieros (Salazar, 2003). Estas tecnologías están integrando al mundo en redes globales, que generan la expansión de diversas comunidades virtuales, reduciendo la distancia social entre gente muy variada, aunque creando barreras muy sutiles e invisibles que suelen aislar a las personas. El ambiente que originan las tecnologías de la información es intangible y virtual; el espacio y el tiempo pierden su significado tradicional y se accede a las personas sin grandes requerimientos y sin proximidad física. Es relativamente fácil obtener información personal a través de la web, pudiendo ser utilizada con diversos propósitos (Smith, 2006). Las sociedades y sus instituciones se ven obligadas a mantener una constante actualización de procesos y herramientas para la transformación de bienes y servicios, a fin de satisfacer exigencias dinámicas; donde las tecnologías suplen los recursos operativos necesarios. Manning (2004) afirma que la explosión tecnológica sucede a la par de rápidos cambios en la economía, que incluyen el crecimiento del comercio virtual en línea y el *outsourcing*, lo cual favorece el desarrollo de una delincuencia económica renovada.

El sector bancario es uno de los que ha experimentado el desarrollo de las nuevas tecnologías, dado que el comercio se ha expandido ilimitadamente por todo el mundo y se realiza de forma electrónica en gran medida. Se crearon en un primer momento máquinas que permitieran realizar transacciones sin necesidad de visitar una agencia bancaria, como en el caso de los cajeros automáticos (ATM) y los puntos de venta automatizados (POS) (Rodríguez, 2000). Luego aparece el banco del ciberespacio, conocido actualmente como la banca electrónica, virtual, on line o e-banking, según la denominación de preferencia (Rincón, 2004; Segistan, 2003; Fernández, 2006).

Según Rincón (2004), existen tres modalidades a través de las cuales las entidades financieras prestan servicios de forma electrónica: la banca en línea, la banca a través de un portal en Internet y la banca en Internet. La primera se refiere al servicio que presta la institución a sus clientes para que puedan acceder a sus cuentas, utilizando un computador y un software especial que le permitirá conectarse a la red de la entidad y ejecutar operaciones como verificación de saldos, pagos y transferencias. La actualización de datos en este tipo

de servicio puede ser deficiente, debido a que los cambios no se introducen en tiempo real y la información puede carecer de precisión. La segunda modalidad, a través de un portal en Internet, implica que el usuario se conecta al establecimiento de crédito sin necesidad de adquirir un software especial, ya que éste se encuentra en el servidor de la institución financiera. Finalmente, la denominada banca en Internet es aquella mediante la cual se eliminan las estructuras tradicionales, prestándose los servicios exclusivamente a través de la red. El ámbito del presente trabajo corresponde al de transacciones a través de un portal de Internet, que denominaremos banca virtual o electrónica. Ella constituye la **banca tradicional** puesta a disposición de los clientes por medios electrónicos o a través de Internet, facilitando un rápido y cómodo acceso a las cuentas para realizar distintas transacciones bancarias, con miras a garantizar un mayor control desde cualquier parte del mundo y a cualquier hora (Segistan, 2003).

La banca electrónica supone dos tipos de servicios: los servicios de información, que consisten en el manejo de datos entre la entidad y el cliente, quien puede consultar sus saldos y movimientos de cuentas, el estado de los préstamos y tarjetas de crédito, entre otros; y los servicios de órdenes, que se refieren a transferencias de fondos, colocación de depósitos, solicitud de tarjetas, chequeras, divisas, etc.

Entre las ventajas que ofrecen las entidades financieras mediante estos servicios se cuentan el ahorro de tiempo y la cobertura, al no requerirse la presencia física del cliente para realizar las transacciones y a la amplitud geográfica que brinda Internet para acceder a los servicios; además de permitir un rápido y sencillo control de las cuentas por parte del cliente. Sin embargo, esta banca virtual conlleva riesgos considerables para la seguridad de la información y algunos derechos de los usuarios, percibidos como carencias en los sistemas tecnológicos y vulnerabilidad de los complejos sistemas informáticos (Smith, 2006). Esto ocurre debido a que mucha de la información sensible viaja a través de la red, lo que permite la usurpación de la identidad, el revelar involuntariamente información confidencial, la difusión y venta de información confidencial no autorizada, los portales falsos o empresas inexistentes y el espionaje, entre otros (Centro Internacional de Estudios Superiores de Comunicación para América Latina, 2001). Por eso Whitaker (1999) señala que *las Nuevas Tecnologías de la Información son un arma de doble*

filo: aumentan nuestras capacidades y nuestro poder, pero también hacen a sus usuarios más vulnerables a la vigilancia y a la manipulación.

Rincón (2004) habla de cuatro tipos de riesgos que corren las entidades bancarias que ofrecen servicios electrónicos: operacional, reputacional, legal y transaccional. El riesgo operacional recae sobre la seguridad y confidencialidad de la información, por deficiencias significativas en la integridad del sistema, quedando expuestos, tanto el banco como su clientela, a accesos no autorizados. Este tipo de riesgo puede presentarse por deficiencias en el sistema de seguridad, falta de políticas de gestión de riesgo, falta o insuficiencia de tecnología, falla en los servicios del proveedor o falta de precaución por parte del cliente, asociándose a la introducción de virus, robo de datos, fraudes y otros ataques (Segistan, 2003; Rincón, 2004). El riesgo reputacional consiste en la publicidad negativa sobre el banco o cualquiera de sus productos o servicios, o para el sector en general, cuando se presentan frecuentes carencias o fallan los sistemas de seguridad. El riesgo legal aparece cuando se viola o se incumple alguna disposición legal, o cuando los derechos y obligaciones de las partes en las operaciones electrónicas no se encuentran bien definidos, lo cual genera incertidumbre y falta de confianza para hacer uso de este tipo de operaciones. Finalmente, el riesgo transaccional implica la falla en el cumplimiento de las obligaciones contraídas, especialmente por el control y manejo de los requerimientos operacionales a nivel internacional, dado que las exigencias legales varían de un país a otro.

El riesgo operacional es uno de los más difíciles de manejar, debido a que los mismos avances tecnológicos crean diversas posibilidades de ataque a los sistemas informáticos de las entidades bancarias y, por tanto, a las cuentas de sus clientes. Rápidamente se hacen obsoletos los sistemas de seguridad más sofisticados que puedan haberse implementado y los ataques más frecuentes son realizados por piratas informáticos o por los mismos empleados del banco. Las personas, singulares o en organizaciones delictivas, efectúan la denominada pesca electrónica (*phishing)*, emplean troyanos o simulan portales (*pharming)*, que son las principales formas para la obtención de información sensible a través de la red (Fernández, 2006; Wüeest, 2005; Delitosinformaticos.com, 2006). El común denominador es la captura del nombre de usuario y la contraseña, lo cual permite el acceso a los sitios web de la entidad financiera o a puntos de comercio electrónico (Fernández, 2006).

Para el manejo de estos riesgos se ha recomendado verificar y actualizar las políticas de seguridad de los bancos, analizar los protocolos de seguridad y los sistemas de encriptación, incorporar contrafuegos (*firewalls*) tanto en los servidores del banco como en los computadores de los clientes, así como la instrucción de los clientes por parte del banco sobre la utilización de sus claves de acceso y la importancia de garantizar la confidencialidad de la misma: ser cuidadoso (Smith 2006).

Las particularidades del desarrollo de las tecnologías de la información han conformado, pues, un entorno impersonal, anónimo, que no requiere desplazamiento físico y en plena expansión en cuanto a la victimización para diversas modalidades delictivas. Los avances tecnológicos de las últimas décadas se han incorporado al ámbito delictivo, al igual que en muchas otras áreas, buscando constantemente la optimización de los recursos para el mejor desarrollo de sus actividades y aprovechando su amplia difusión y disponibilidad.

Los delitos evolucionan a la par de todas las estructuras sociales, exigiendo adecuación de políticas para su control. El fraude electrónico bancario, tipificado en la legislación especial vigente (Ley Especial contra Delitos Informáticos, 2001 y Ley General de Bancos y otras Instituciones Financieras, 2001) aparece como una lesión jurídica cuya documentación e interpretación requiere intervención especializada e interdisciplinaria. Ello se debe a que es preciso integrar conocimientos y experiencias de diversos ámbitos para tener una visión completa del fenómeno, en un medio caracterizado por la virtualidad y la ocultación de los signos de identidad inmediata.

El delito de fraude, como ejecución de transferencias fraudulentas, implica el traslado de montos de dinero desde la cuenta de un titular hacia las cuentas de terceros, para luego retirar el producto de la defraudación, generalmente a través de las propias taquillas del establecimiento bancario. El núcleo de este fraude radica en que quien realiza la transferencia pretende ser el titular de la cuenta afectada, cuando manipula códigos o claves que le permiten un acceso indebido. El control bancario supondría identificar rápidamente dicha suplantación para detener la transacción en curso. Se ha llegado a describir este delito como *de oportunidad especial, ya que su comisión se realiza al presentarse el momento más favorable (Guerrero y Santos, 1993).* Las entidades bancarias y financieras se han visto en la nece-

sidad de actualizar continuamente sus servicios, incorporándolos a la tecnología informática, no solo para brindar mayores facilidades a sus clientes, sino para controlar la comisión de delitos. Sin embargo, los mecanismos de protección reducen su efectividad cuando la información requerida para lograr el fraude es suministrada por los propios clientes, por personas cercanas al cliente, como familiares, socios o amigos, o por funcionarios de la propia institución bancaria, antiguos o activos, quienes manejan *información sensible sobre claves, procedimientos y parámetros de disponibilidad y uso de fondos sobre las cuentas de los clientes*.

En este artículo se describen los resultados de un estudio que ha permitido aproximarse a las variables asociadas a la comisión del fraude electrónico utilizando los mecanismos disponibles por la banca virtual. Nuestra atención se ha centrado en las condiciones situacionales y personales que favorecen la ejecución de fraudes mediante transferencias electrónicas de fondos, a través de la revisión de los procesos de supervisión, detección, intervención y control aplicados por la institución bancaria. Así, nos hemos aproximado a información sobre los fraudes bancarios que no estaba disponible hasta ahora, explorando alternativas de control del fraude que se centren en los procesos y las oportunidades para la defraudación, antes que en las disposiciones, actitudes o intereses de los infractores, si bien no negamos la importancia de estos últimos aspectos.

La revisión sumaria del fraude en la banca virtual venezolana, a través de los datos de que dispone una de las entidades bancarias del país, indica una incidencia significativa del delito de fraude electrónico a través de los servicios en línea que ofrecen las instituciones financieras. La información sugiere que, en la mayoría de las oportunidades (entre 60% y 90% de las veces), el fraude es exitoso en términos del apoderamiento del dinero sustraído. También se ha registrado un incremento de la defraudación en el primer trimestre de 2006 en comparación con el trimestre equivalente de 2005. Además, se ha sugerido un patrón delictivo para la movilización electrónica fraudulenta, a través de internet, mediante la creación o modificación del perfil de un cliente en la banca virtual, a fin de transferir fondos que se retiran por las taquillas del banco, los cajeros automáticos (ATM) o los puntos de venta (POS) (Umbría, 2006).

En relación con el proceso ejecutivo del delito, se realizó un análisis de exposición al riesgo inherente al proceso de fraude electrónico y uno relativo al cliente. En cuanto al primero, se encontró que las tres cuartas partes de los casos de transferencias fraudulentas fueron detectadas mediante mecanismos de monitoreo de la transacción y que, en una cuarta parte de los casos, se logró retirar por taquillas fondos superiores al umbral de activación de la alarma fijada por el banco. En cuanto al riesgo vinculado al cliente, se observó que suelen ser más atacados aquéllos que utilizan la banca virtual y que disponen de una sola clave para el uso de los cajeros automáticos y para las operaciones telefónicas y de Internet. La disponibilidad de un perfil del usuario de la banca virtual no parece ser de gran relevancia para prevenir el fraude debido a que se puede crear un perfil falso o modificar el existente (Umbría, 2006).

Esta información, conjuntamente con la obtenida mediante grupos focales con gerentes y representantes bancarios entre 2002 y 2003 (Gabaldón y Moreno, 2003) sugiere la fuga de información sensible, bien a través de personal activo del banco o de ex empleados o allegados a éstos, así como la cuestión del favorecimiento de la defraudación por la falta de cuidado por parte de las víctimas y la influencia de la generalización de las transacciones electrónicas y del desarrollo tecnológico en diversas modalidades de defraudación.

Los datos hasta ahora disponibles permiten destacar la importancia de profundizar en el estudio de modalidades delictivas que evolucionan a la par de la tecnología y de los cambios en los modos de desarrollarse las operaciones bancarias. La investigación que se adelante al respecto permitirá determinar el peso de determinadas variables en la defraudación, así como adquirir y renovar conocimientos, técnicas y herramientas para prevenir, controlar e intervenir frente a la expansión del fenómeno delictivo informático.

2. LA PERSPECTIVA DE LAS OPORTUNIDADES DELICTIVAS Y SU APLICACIÓN A LAS TRANSFERENCIAS ELECTRÓNICAS BANCARIAS

En los últimos veinticinco años, diferentes investigadores abocados al estudio de la delincuencia aportaron conceptos y perspectivas teóricas que replantearon los análisis tradicionales sobre las características del delincuente y de las víctimas. Estos aportes sugirieron la concentración en la

situación y en los elementos del entorno que pudieran propiciar o facilitar la comisión de un acto delictivo. De allí surgen las teorías situacionales sobre el delito, estrechamente vinculadas a la perspectiva de la escogencia racional de la delincuencia, según la cual el delito se concibe como conducta instrumental encaminada a satisfacer necesidades del delincuente (entre las cuales está, aunque no exclusivamente, el dinero) mediante la adopción de decisiones limitadas por el tiempo y la disponibilidad de información relevante, siendo que esta información se circunscribe, de ordinario, a las situaciones y circunstancias inmediatas al acto (Clarke, 1995: 98). Esta perspectiva dio lugar la formalización de las denominadas teorías de las oportunidades delictivas, que han sido recogidas y sintetizadas por Birkbeck (1984-1985), donde se enfatiza el concepto de oportunidad para el delito y se analizan los postulados y supuestos que se han planteado al respecto.

Birkbeck encontró en su revisión dos enfoques fundamentales. Uno de ellos centrado en el denominado "análisis del riesgo de la victimización", donde se consideran esenciales las características del modo de vida del delincuente y la víctima, que los acercan o distancian facilitando la victimización; y el otro basado en los elementos constitutivos de la oportunidad para el delito, esto es, un blanco accesible y escasas probabilidades de detección y detención del delincuente. En ambas perspectivas, la motivación del delincuente se supone constante y no es un tema de análisis específico. De la evaluación de las teorías, se ha sugerido que no presentan una exposición completa y explícita de su estructura y contenido, ni una identificación clara de sus conceptos y proposiciones; además, son escasos los datos disponibles para guiar las formulaciones de sus postulados y para facilitar la contrastación empírica de las proposiciones que establecen relaciones entre características de la víctima y las dimensiones de riesgo que favorecen la victimización (Birkbeck y Lafree, 1989).

Luego del análisis crítico de estas formulaciones teóricas, se ha intentado una definición concreta de la oportunidad para el delito, que faltaba en las teorías revisadas, aparentemente, porque se suponía *obvia y carente de interés,* bajo el argumento de que ella sería una condición necesaria pero no suficiente para que ocurriera el delito (Birkbeck, 1984-1985:45). Así pues, una oportunidad para cometer el delito es cualquier situación en la cual los recursos del delincuente superan los recursos para la protección de un deter-

minado objeto (Birkbeck, 1984-1985: 58), donde los primeros facilitan la comisión del acto delictivo mientras los segundos la obstaculizan.

En un artículo más reciente (Warr, 2001) se retoma la idea de que la oportunidad es una *condición necesaria pero no suficiente*, justificando la importancia de estudiar el delito desde una perspectiva integral. La oportunidad, entendida de este modo, permite concebir la conjunción de situaciones favorables a la comisión delictiva, como agregado, e incluso explorar en qué medida los delincuentes maximizan sus posibilidades de éxito mediante la búsqueda de ambientes más idóneos. En este sentido, las oportunidades serían múltiples (Warr, 2001: 70 y 78). Otra perspectiva reciente ha pretendido relativizar el concepto de oportunidad, considerando que la relevancia que ésta puede tener depende de los deseos y compromisos de la persona, esto es, de su entorno moral (Wikström, 2006: 535). Dentro de estas perspectivas, el concepto oportunidad pierde relevancia central en la explicación de la conducta delictiva y resulta difícil de operacionalizar a los efectos de la investigación empírica. Por ello, adoptaremos el concepto sintético propuesto por Birkbeck (1984-1985), como condensación en una sola situación de recursos para la comisión frente a recursos para la protección, y la posibilidad de balancear unos y otros, que parece más apropiado para una aproximación al estudio de modalidades de defraudación, donde dicha ponderación puede resultar crucial para determinar el éxito o fracaso de la actividad delictiva. De este modo, adoptaremos la definición y el planteamiento de Birkbeck sobre la oportunidad delictiva.

En las teorías de las oportunidades para el delito resultan importantes el acceso que logre el delincuente al objeto o a la víctima, elemento que ha sido asociado a la proximidad física y al contacto que exista entre uno y otra, las posibilidades de evadir las consecuencias aversivas del acto y las características de la víctima. Es dentro de esta perspectiva criminológica que se ha planteado la defraudación electrónica a los efectos de esta investigación, bajo un modelo en el cual los principales elementos a considerar guardan relación con el *valor del objeto de la defraudación*, por una parte, y con los recursos de que disponen el delincuente y la eventual víctima, para cometer el delito o para proteger el objeto de la defraudación, respectivamente. Precisamente de la disparidad entre recursos del delincuente para la comisión y de la víctima para la protección, surge el concepto de la *magni-*

tud de la oportunidad. En esta investigación no hemos abordado los recursos del delincuente, pues su estimación no es factible mediante un seguimiento de las transacciones denunciadas como fraudulentas a través de la unidad de investigación de fraudes del Banco. Sin embargo, no descartamos su incorporación dentro del modelo de análisis en fases sucesivas mediante una metodología que permita describirlos y ponderarlos.

3. CONCEPTOS, VARIABLES E HIPÓTESIS DE LA INVESTIGACIÓN

La investigación adelantada pretende evaluar el *valor* y la *magnitud* de la oportunidad para ejecutar el fraude electrónico, considerando el ambiente de las tecnologías de la información. A diferencia de la delincuencia convencional, donde la aproximación física y la fragmentación temporal son fundamentales, mediante estas tecnologías se genera un entorno de ejecución sin desplazamiento físico del delincuente y mediante condensación temporal e, incluso, simultaneidad. Por ello, se pretende realizar un análisis de determinados indicadores que permitan la medición de las mencionadas variables en este nuevo contexto y su incidencia en la victimización.

Esta situación obliga a definir con mayor detenimiento cada variable y a establecer cuidadosamente los indicadores que permitan medir el fenómeno, lo que a su vez contribuye a la actualización de las perspectivas criminológicas fundamentadas en el enfoque de las oportunidades para el delito. En este sentido, resulta conveniente examinar las variables relacionadas con los elementos encontrados en la definición propuesta por Birkbeck (1984-1985) sobre oportunidad para el delito, para determinar su alcance y aplicación al medio virtual.

Las dimensiones del riesgo, concebidas como contacto (o frecuencia de evaluación del blanco por parte del delincuente), protección (o nivel de seguridad frente al acto delictivo) y valor (o beneficio derivado del blanco atacado) (Birkbeck, y Lafree, 1989: 20), requieren un replanteamiento en el medio virtual; ello se debe a que la evaluación del delincuente puede ser más ampliamente extendida a un número mayor de víctimas potenciales, a que la protección implica concurrencia de recursos personales e institucion-

ales y a que el valor podría registrar menor variación cualitativa, por cuanto los montos defraudables representan sumas variables de dinero en cuentas bancarias.

3.1. Variables dependientes

La variable dependiente, es decir *lo que se pretende explicar*, es la situación de defraudación, que se puede distinguir en diversos momentos y modalidades. En este sentido, hemos distinguido tres condiciones de la victimización, que corresponden al traslado de los fondos (vitimización inicial), al aprovechamiento final (o victimización terminal) y a la probabilidad de victimización reiterada (o victimización múltiple), que definimos de la siguiente manera:

Victimización inicial (consumación del fraude). Esta variable se refiere al perfeccionamiento jurídico del fraude que, según el artículo 14 de la Ley Especial contra los Delitos Informáticos (Venezuela, 2001a), se produce desde el momento en el cual se insertan las instrucciones falsas para movilizar el dinero. Este momento de consumación corresponde a la transferencia de determinado monto de dinero de una cuenta a otra, y para cuya estimación mediremos el valor del monto afectado y la magnitud del daño causado. Llamaremos esta variable *monto expuesto*, en virtud de la denominación establecida por el banco para el dinero que es objeto de la defraudación y se encuentra temporalmente en la cuenta receptora. La variable asume tres categorías: Menos de Bs. 1 millón, hasta Bs. 5 millones y Más de Bs. 5 millones. El monto expuesto será también tratado como variable independiente al analizar el comportamiento del aprovechamiento final y de la probabilidad de victimización reiterada.

Victimización terminal (agotamiento del fraude). Si bien se entiende que el fraude se consuma una vez realizada la transferencia electrónica de una suma de dinero en perjuicio del titular de una cuenta bancaria, el delito no se ha agotado hasta que ese dinero no sea retirado de la cuenta receptora (por taquilla, cajeros automáticos o puntos de venta), debido a que queda abierta la posibilidad de que el banco revierta la operación y se recuperen los fondos, caso en el cual el delito se considerará frustrado. Por ello, resulta relevante indagar sobre los factores asociados al aprovechamiento final (o agotamiento del fraude) y lo trataremos como una variable dependi-

ente en un segundo momento, que denominaremos *resultado final del fraude*, con dos categorías posibles: frustrado (recuperación total o parcial del monto expuesto) y agotado (pérdida total).

Victimización múltiple (reiteración) Esta situación se plantea debido a la posibilidad de que una misma víctima sea defraudada reiteradamente, por lo cual se distinguen, en cuanto a la modalidad de la victimización, dos categorías: única o singular y múltiple.

3.2. Variables independientes

Las variables independientes básicas de la presente investigación, es decir, las condiciones *que explican el fraude*, son las que hemos definido como valor y magnitud de la oportunidad para la transferencia electrónica indebida. A partir de ellas, hemos formulado algunas hipótesis respecto a las probabilidades de consumación y agotamiento del fraude electrónico, y hemos establecido los indicadores que permitan medir dicha probabilidad.

3.2.1. Valor de la oportunidad

El valor representará la ganancia o beneficio probable que el defraudador estima obtener con la ejecución de la transferencia fraudulenta, lo cual puede orientar, en principio, la escogencia del blanco dentro de una racionalidad utilitarista. Motivado el delincuente por tal beneficio, su primer criterio de evaluación es la percepción de la dimensión de la ganancia a ser obtenida con la victimización. Por consiguiente, formulamos la hipótesis, conforme a la teoría, de que *a mayor cantidad de dinero en una cuenta, mayor el valor de la oportunidad y, en consecuencia, mayor probabilidad de que esa cuenta sea el blanco del delito*. Los indicadores de valor son el *monto disponible en la cuenta* para el momento del fraude y el *segmento* al que pertenece el titular de la cuenta según la clasificación del banco.

3.2.2. Magnitud de la oportunidad

En cuanto a la magnitud de la oportunidad para el delito de fraude electrónico bancario, que constituye la disparidad entre recursos del delincuente y recursos de protección, hemos construido las siguientes hipótesis:

a) A menor supervisión de la cuenta, mayor probabilidad del fraude. La supervisión se refiere a la vigilancia o frecuencia de monitoreo que el

titular de la cuenta esté practicando sobre ella. Se asume que menor supervisión disminuye la protección del objeto.

b) A menor movimiento de las cuentas, mayor probabilidad del fraude. El movimiento de las cuentas se encuentra relacionado con la supervisión, asumiendo que se pueden registrar diversos grados de supervisión dependiendo del tipo de cuenta del que se trate. En la medida que una cuenta registra menores movimientos, ello sugiere menor acceso del titular y, por consiguiente, menor protección del objeto.

c) A mayor información que el defraudador posea sobre el titular de la cuenta, mayor probabilidad del fraude. La información indispensable requerida para el fraude está representada, principalmente, por el número de la cuenta, los datos de identificación del titular, claves de acceso a cajeros automáticos y banca virtual, y montos disponibles en la cuenta. En la medida en que se difunde mayor información sensible sobre las cuentas, disminuye la protección del objeto.

d) A menor número de claves de acceso a las cuentas, mayor probabilidad del fraude. Se asume que hay más cuidado con las cuentas cuando se dispone de claves múltiples, por cuanto se utilizaría una de ellas para las operaciones de Internet y otra para efectuar retiros a través de cajeros automáticos. Esto hace más complejo el proceso de transferir y retirar fondos, elevando el nivel de protección del objeto.

e) A mayor ejecución de la transferencia en tiempo no laborable, mayor la probabilidad del fraude. Se asume que una vez activadas las alertas parametrizadas, opera un seguimiento bancario, que incluye contactos con el cliente para verificar la transacción. Si la transferencia se hace en tiempo no laborable, este seguimiento y contactos son más improbables. Todo ello favorece la extensión del tiempo entre la ejecución de la transferencia y la obtención del beneficio final mediante el retiro del dinero.

f) A menor activación de las alertas parametrizadas, mayor la probabilidad del fraude. Esto **s**upone que, cuando la transferencia se haga por montos menores al umbral de desencadenamiento de la alerta, tales alarmas no se activarán, bajando el nivel de protección.

g) A menor observancia de las pautas de control de operaciones de la institución bancaria, mayor probabilidad del fraude. Suponemos que, según la ubicación geográfica y jerárquica de la oficina donde se hace el retiro producto de la transferencia fraudulenta, podrían registrarse menores o mayores niveles de protección, debido al posible incremento del cuidado y capacitación del personal, así como de la eficiencia operativa, en agencias centrales o muy concurridas. La verificación de esta hipótesis permitiría observar si los defraudadores prefieren agencias con ciertas particularidades que favorezcan las probabilidades de éxito.

Los indicadores establecidos para evaluar la magnitud de la oportunidad en el fraude electrónico bancario son: la supervisión de la cuenta por parte del titular (tipo de cuenta, tiempo de detección del fraude), el acceso a información sensible sobre el mismo (llamadas o correos electrónicos), el cuidado que el titular tenga sobre sus cuentas (número de claves, disponibilidad de perfil virtual), el tiempo en el cual se consuma y se agota el fraude (día y hora de transferencia y retiro), la probabilidad de activación de las alertas parametrizadas (activación y monto expuesto) y el cumplimiento de pautas establecidas por el banco para el pago de dinero en sus oficinas (ubicación geográfica y tipo de oficina en la que se retiran los fondos).

3.2.3. Variables demográficas

La teoría de las oportunidades delictivas permite adelantar algunas hipótesis vinculadas a las dimensiones de riesgo que guardan relación con las características personales de las víctimas. Por ello, hemos decidido incorporar al análisis cuatro de dichas características, frente a las cuales realizamos las siguientes proposiciones.

Edad. Partiendo del supuesto de que las personas jóvenes manejan con mayor facilidad, tal vez destreza, las herramientas informáticas disponibles, podríamos suponer mayores niveles de protección entre los jóvenes, quienes podrían estar mayormente atentos que las personas maduras frente a eventuales ataques. Por consiguiente, suponemos que *a medida que aumenta la edad de los titulares de las cuentas, aumenta el riesgo de victimización.*

Sexo. Se busca conocer si las titulares del sexo femenino son más cuidadosas con el estado de sus cuentas que los clientes del sexo masculino, incrementando, mediante la supervisión, sus niveles de protección. Asu-

miendo esta diferencia, suponemos que *las mujeres tienden a ser menos victimizadas que los hombres en materia de fraude electrónico.* Los estudios de victimización reportan, en general, una menor victimización de las mujeres que de los varones, aunque para las estafas las diferencias se reducen considerablemente (Gabaldón, Benavides y Parra, 2007: 322).

Nivel Educativo. Se puede suponer que el grado de instrucción del titular guarda relación con la probabilidad de supervisión de las cuentas, si se asume que comporta mayores destrezas informáticas, incrementando así el nivel de protección. Por consiguiente, suponemos que *a mayor nivel educativo del cliente, disminuye el riesgo de victimización*.

Ocupación. Se pretende estimar si suelen ser más cuidadosos con sus cuentas los profesionales, empresarios y comerciantes, que personas con otras ocupaciones (amas de casa, estudiantes, obreros, entre otros), debido al contacto que con sus cuentas mantienen en función de la actividad económica que desempeñan, lo cual incrementaría el nivel de supervisión y, por ende, de protección. Por consiguiente, suponemos que *los profesionales, empresarios y comerciantes serán menos victimizados que los representantes de otras ocupaciones.*

4. RESULTADOS

El proceso de recolección de datos se inició en septiembre de 2006, a través del registro de información proveniente de varias bases de datos del banco y de los expedientes correspondientes a cada caso de fraude considerado procedente por los encargados de la investigación, en el período mayo 2004 - agosto 2006. Con este proceso, se identificaron 226 titulares afectados por transferencias fraudulentas bajo la modalidad de *pagos a terceros*. No obstante, fueron excluidos seis casos por haberse determinado que obedecían a errores del cliente no fraudulentos, o porque correspondían a titulares afectados con la condición de personas jurídicas, lo que ocasionaría una distorsión de los resultados.

El total de transacciones fraudulentas investigadas y útiles para ser procesadas con el programa estadístico SPSS (*Statistical Package for the Social Sciences*) fue de 417 casos correspondientes a 220 clientes victimiza-

dos una o más veces. La pluralidad de victimización dificulta el análisis de las variables, debido a que las características personales se repiten en varios casos en más de una oportunidad. Por tal motivo, creamos dos bases de datos, una en función del número de transferencias fraudulentas (417 casos), con la que se medirían las variables situacionales de cada una; y otra en función del número de clientes afectados (220 casos) para la medición de variables referidas a características de las cuentas afectadas y sus titulares. De este modo, los análisis estadísticos se realizan paralelamente sobre las dos bases de datos disponibles, dependiendo de las variables que se requiera describir y contrastar.

4.1. Variables situacionales y personales asociadas a la consumación del fraude

Para verificar las hipótesis planteadas en este trabajo, realizamos, en principio, análisis estadísticos bivariados o pruebas de discrepancia, a través de los cuales comparamos las variables independientes, mediante sus indicadores, con las variables dependientes, para determinar si existe asociación estadísticamente significativa entre ambas. De los resultados obtenidos, se pudo concluir que el valor de la oportunidad es la variable que encuentra una asociación más consistente con la defraudación electrónica

4.1.1 Valor de la oportunidad y fraude

A medida que se incrementa el monto disponible en cuenta, aumentan el monto expuesto (X^2= 113,74, p<0,001) y la probabilidad de victimización múltiple (X^2= 18,07, p=0,001). A medida que el segmento a que pertenece el afectado progresa desde el nivel más bajo hasta el más alto, se incrementa también el monto expuesto (X^2=60,00, p<0,001). Sin embargo, el segmento no guarda relación con el tipo de victimización (singular o múltiple). Así pues, los datos sugieren confirmación de la proposición general de que a mayor valor de la oportunidad, más probable es el fraude.

4.1.2. Magnitud de la oportunidad y fraude

A menor supervisión de la cuenta, mayor probabilidad del fraude.

La menor disponibilidad de perfil virtual del cliente se encuentra asociada a mayor monto expuesto en el fraude (X^2=19,36, p<0,001), aunque no a la victimización múltiple. A medida que aumenta el tiempo transcurrido

entre la transferencia fraudulenta y su detección, aumenta la probabilidad de agotamiento del fraude (X^2= 20,72, p<0,001), aunque no la victimización múltiple. Estos resultados apoyan en gran medida nuestra hipótesis cuando nos referimos a la consumación y al agotamiento del fraude.

A menor movimiento de las cuentas, mayor probabilidad del fraude.

No hay relación lineal entre los tipos de cuentas bancarias afectadas por la transacción fraudulenta (ahorros, máxima, corriente, nómina, fideicomiso) y el monto expuesto o el tipo de victimización, lo que sugiere el rechazo de nuestra hipótesis. Además, se obtuvo que las cuentas corrientes, que deberían contar con mayor supervisión debido a sus movimientos y a la necesidad de conciliación para no emitir cheques sin respaldo, son más vulnerables a las transferencias fraudulentas por encima de Bs. 1.000.000. Esto podría deberse a que, teniendo las cuentas corrientes mayor número de operaciones que las de ahorro, el defraudador supone que la detección rápida de una transacción determinada, incluyendo la fraudulenta, es menos probable.

A mayor información que el defraudador posea sobre el titular de la cuenta, mayor probabilidad del fraude.

No existe asociación entre frecuencia de llamadas telefónicas o correos electrónicos dirigidos a los clientes y el monto expuesto o el tipo de victimización. Este resultado contradice, aparentemente, nuestra hipótesis y la suposición de que el phishing constituye uno de los principales factores de riesgo para la defraudación, aunque podría deberse a que los clientes no desean informar sobre este tipo de contactos a los investigadores del banco, por temor a desmejorar su posición frente al reclamo.

A menor número de claves de acceso a las cuentas, mayor probabilidad del fraude.

La disposición de mayor número de claves no previene, aparentemente, la comisión de fraudes, medida por el monto expuesto; por el contrario, en su presencia tienden a aumentar los fraudes por arriba de Bs. 1.000.000. Ello contradice la hipótesis del incremento de protección, representado por más de una clave, en la comisión del fraude. No hay relación entre número de claves y tipo de victimización (singular o múltiple).

A mayor ejecución de la transferencia en tiempo no laborable, mayor la probabilidad del fraude.

Los días finales de la semana (jueves a domingo) están más asociados a las transferencias fraudulentas que los iniciales (lunes a miércoles) (X^2= 4,55, p< 0,04). Los retiros de los fondos (agotamiento) tienden a concentrarse en los primeros días de la semana (X^2=10,38, p=0,006). Esto podría suponer que hay una motivación temporal para cometer el fraude, que apoya nuestra hipótesis, debido a que realizando las transferencias los días finales de la semana, hay menor probabilidad de activación operacional del banco y, por tanto, mayor oportunidad para retirar el dinero a principios de la semana. Por otro lado, es más probable el agotamiento cuando se realizan retiros fraccionados.

A menor activación de las alertas parametrizadas, mayor la probabilidad del fraude.

Se observa una tendencia al incremento del monto expuesto en el rango de Bs. 1.000.000 a Bs. 5.000.000, en la medida en que no se activan las alertas (X^2= 56,86, p< 0,001). Se observa, además, una relación inversa entre montos expuestos (por arriba de Bs. 5.000.000) y el agotamiento de los fraudes (X^2=4,64, p =0,03). Ello podría sugerir que las alertas parametrizadas inciden en menor cantidad de fraudes agotados, si consideramos que por encima de Bs. 5.000.000 se deberían desencadenar las alertas parametrizadas, lo que permitiría confirmar nuestra hipótesis. Sin embargo, la prueba de discrepancia entre activación de alertas y el agotamiento del fraude no muestra asociación significativa entre ambas variables y ello nos lleva a considerar que la hipótesis planteada en esta investigación respecto a la activación de alertas, encuentra solo respaldo parcial en los resultados y que requiere mayor investigación.

A menor observancia de las pautas de control de operaciones de la institución bancaria, mayor probabilidad del fraude.

Las agencias de mayor rango, donde se encuentran las Gerencias Regionales, parecieran ser menos propensas al agotamiento del fraude, que las que le siguen: agencias tipo A y B. La categorización de las sucursales bancarias corresponde a un indicador combinado de superficie y recursos hu-

manos en cada oficina, de modo que las mejor dotadas se encuentran en el tope. Por otra parte, parece haber una incidencia mayor de dicho agotamiento en el Distrito Capital comparado con otras regiones del país. Se ha observado también una mayor incidencia del fraude agotado cuando se utiliza la vía de Internet que cuando se utiliza el centro de atención telefónica (X^2= 7,27, p<0,03), lo cual sugiere que los controles personalizados podrían tener un efecto en la minimización del agotamiento de los fraudes. No obstante, dado que los retiros por taquilla no superan el 40%, no se puede hacer ninguna inferencia sobre el peso de los controles personalizados en las oficinas bancarias.

4.1.3. Variables demográficas y fraude

La edad, el sexo, el nivel educativo y la ocupación muestran algunas asociaciones estadísticas con la consumación del fraude (monto expuesto), aunque no con el tipo de victimización (singular o múltiple). Sin embargo, luego de explorar la asociación entre las variables de valor (monto disponible en cuenta y segmento del titular afectado) y las variables demográficas, se ha determinado una asociación entre ambas. Ello permite suponer que las variables demográficas no tienen peso autónomo como indicadores de niveles alternativos de protección, sino que son covariantes con las de valor que se han mostrado fuertemente asociadas al fraude.

4.2. Hacia un modelo sobre consumación, victimización múltiple y agotamiento del fraude electrónico

El análisis multivariado pretende explorar el peso relativo de diversas variables asociadas a la comisión del fraude. Las variables independientes son las que tienen posible valor explicativo en el resultado, mientras las variables dependientes son los resultados mismos. Son variables independientes en nuestra investigación, los indicadores de valor y magnitud de la oportunidad antes explicados, así como las variables demográficas (edad, sexo, nivel educativo y ocupación). Son variables dependientes: a) la consumación del fraude, medida por el monto expuesto, es decir, la cantidad de dinero que ha sido afectada por la transacción fraudulenta; b) el resultado final del fraude, medido por la condición de haberse perdido o no la totalidad del dinero afectado por la transacción fraudulenta; y c) el tipo de victimización, medida por la condición de victimización singular o múltiple.

Para efectuar el análisis multivariado seleccionamos las variables independientes que mostraron tener alguna asociación con las variables dependientes mediante el análisis bivariado, anteriormente descrito. Este análisis multivariado utiliza la técnica de la regresión logística, mediante la cual se efectúa una ecuación de regresión de las variables independientes contra la variable dependiente, que asume la condición de categórica y dicotómica, esto es, sus valores no son continuos y se distribuyen entre dos posibilidades únicamente.

La consumación del fraude fue dicotomizada en monto expuesto menor a Bs. 5.000.000 y mayor a Bs. 5.000.000. El tipo de victimización fue dicotomizado en singular (cuando no se ha repetido para el mismo titular) y múltiple (cuando se ha registrado más de un caso para el mismo titular). El agotamiento del fraude fue dicotomizado en frustrado (recuperación total o parcial del monto expuesto) y agotado (pérdida total del monto expuesto).

La Tabla 1 muestra los resultados del análisis multivariado para la variable dependiente consumación (monto expuesto) y las variables independientes monto disponible en cuenta (con cinco categorías: hasta Bs 1.150.000; desde Bs. 1.150.001 hasta Bs. 3.225.000; desde Bs. 3.225.001 hasta Bs. 7.330.000; desde Bs. 7.3330.001 hasta Bs. 21.350.000; y más de Bs. 21.350.000), segmento de pertenencia del cliente (con tres categorías: bajo, medio y alto), disponibilidad de perfil virtual (con dos categorías: sí o no), activación de alertas parametrizadas (con dos categorías, sí o no), sexo (varón/hembra), edad (18-32; 33-42; 43-55; >55), ocupación (profesionales y gerentes, empleados y otros) y nivel educativo (primaria, secundaria, técnico, universitario y postgrado).

Como se puede apreciar, el monto disponible en cuenta se encuentra fuertemente asociado con el monto expuesto (B= 0,94, p= 0,000), lo cual indica que a medida que aumenta el primero, se incrementa también el segundo. Esto sugiere que el defraudador parte del conocimiento de los montos disponibles por los titulares para apuntar a magnificar la defraudación, así que el valor de la oportunidad es el primer predictor de la comisión delictiva.

Tabla 1
Variables Asociadas a la Consumación del Fraude Electrónico

Variable	B	E.T.	Wald	gl	Sig.	Exp (B)
Monto Disponible en Cuenta	0,937	0,214	19,158	1	0,000	2,552
Segmento del Titular	0,278	0,353	0,619	1	0,431	1,32
Disposición de Perfil Virtual	0,458	0,493	0,864	1	0,353	1,581
Activación de Alertas	0,004	0,027	0,021	1	0,886	1,004
Sexo del Titular	-0,199	0,591	0,113	1	0,736	0,820
Edad del Titular	-0,127	0,247	0,264	1	0,607	0,881
Ocupación del Titular	-0,004	0,317	0,000	1	0,989	0,996
Nivel Educativo del Titular	-0,027	0,256	0,011	1	0,915	0,973
Constante	-0,5388	1,906	7,990	1	0,005	0,005

La no disponibilidad de perfil virtual (B= 0,46) y el incremento del segmento del cliente (B= 0,28) registran asociación positiva con el incremento del monto expuesto, aunque la relación no es estadísticamente significativa. Las variables demográficas no muestran asociación relevante con la exposición al fraude dentro del modelo multivariado.

La Tabla 2 muestra los resultados del análisis multivariado para la variable dependiente tipo de victimización (singular/múltiple) y las variables independientes monto disponible en cuenta, segmento de pertenencia del cliente, sexo, edad, ocupación y nivel educativo.

Nuevamente el monto disponible en cuenta se encuentra fuertemente asociado al tipo de victimización, aumentando la probabilidad de reiteración de esta última a medida que aumenta el monto disponible (B=0.46, p= 0.000). Esto indica que las víctimas son atacadas en forma sucesiva más probablemente a medida que se eleva su disponibilidad monetaria, lo cual sugiere que los ataques obedecen a una evaluación sustanciada del valor de la oportunidad. El segmento de pertenencia del cliente no guarda relación con esta probabilidad, lo que confirma que una suposición genérica sobre la capacidad económica de la víctima no es lo determinante, sino la identificación precisa del monto a ser apropiado. Las mujeres (B= -0.50) y los de me-

Tabla 2
Variables Asociadas a la Victimización Múltiple en el Fraude Electrónico

Variable	B	E.T.	Wald	gl	Sig.	Exp (B)
Monto Disponible en Cuenta	0,455	0,131	12,143	1	0,000	1,576
Segmento del Titular	0,048	0,261	0,033	1	0,856	1,049
Sexo del Titular	-0,500	0,395	1,599	1	0,206	0,607
Edad del Titular	-0,052	0,170	0,095	1	0,758	0,949
Ocupación del Titular	-0,015	0,220	0,004	1	0,947	0,986
Nivel Educativo del Titular	-0,231	0,180	1,646	1	0,200	0,794
Constante	0,349	1,072	0,106	1	0,745	0,706

nor nivel educativo (B=.-0.23) parecieran ser menos victimizados en forma múltiple, aunque los estimados no son estadísticamente significativos. Las restantes variables demográficas no parecen guardar relación con el tipo de victimización singular o múltiple.

La Tabla 3 muestra los resultados del análisis multivariado para la variable dependiente resultado final del fraude (frustrado/agotado) y las variables independientes día de la transacción (lunes-miércoles y jueves-domingo), el día del retiro (lunes-miércoles y jueves-domingo), la zona geográfica de la oficina bancaria donde se efectuó el retiro (Región Capital y Otras), el tipo de agencia bancaria del retiro (Gerencia Regional, Agencias A-B y Otras), el monto expuesto (< Bs. 5.000.000 y > Bs. 5.000.000) y el tiempo transcurrido desde la comisión hasta el reclamo (el mismo día, 1-3 días, 4-6 días, 7-16 días y >16 días)

Como se puede observar, el día del retiro se encuentra fuertemente asociado con dicho agotamiento (B= -0,44, p= 0,000), y el coeficiente negativo indica que durante los tres primeros días es más probable que se disponga de los fondos transferidos. También el tiempo transcurrido entre la comisión y la detección se encuentra fuertemente asociado al agotamiento del fraude: a mayor tiempo, más probabilidad de agotamiento (B= 0.52, p= 0.000). Las restantes variables no guardan asociación estadísticamente significativa con el agotamiento del fraude.

Tabla 3
Variables Asociadas al Agotamiento del Fraude Electrónico

Variable	B	E.T.	Wald	gl	Sig.	Exp (B)
Día de la Transferencia	0,519	0,364	2,036	1	0,154	1,681
Día del Retiro	-0,437	0,063	47,821	1	0,000	0,646
Ubicación de la Agencia de Retiro	-1,461	1,467	0,993	1	0,319	0,232
Tipo de Oficina de Retiro	0,340	0,134	0,087	1	0,768	1,040
Monto Expuesto	-7,216	7,141	1,021	1	0,312	0,001
Tiempo Transcurrido Comisión-Detección	0,524	0,142	13,655	1	0,000	1,688

5. CONCLUSIONES

Los resultados de la presente investigación demuestran la utilidad del enfoque de las oportunidades delictivas para el análisis de variables relacionadas con defraudación bancaria mediante transferencias electrónicas. Si bien dicho enfoque teórico ha sido desarrollado para tipos convencionales de delincuencia predatoria o mañosa, contra las personas o la propiedad, su aplicabilidad al medio de las tecnologías de la información resulta prometedora y podría orientar medidas de prevención y control delictivo orientadas por el enfoque situacional del delito, que pone su atención en las condiciones favorecedoras de la delincuencia antes que en las motivaciones individuales de los delincuentes.

Dentro de la perspectiva de las oportunidades delictivas, los indicadores de valor predicen mejor el fraude electrónico que los indicadores de magnitud de la oportunidad, si tomamos en consideración el peso relativo del monto disponible en la cuenta afectada en relación al monto expuesto. Las asociaciones estadísticas entre el monto disponible en la cuenta y el segmento del cliente, por una parte, y el monto expuesto, por la otra, son altamente significativas, así como también lo es la relación entre el monto disponible y la probabilidad de victimización múltiple. También dentro del modelo multivariado de análisis, el monto disponible es la variable que mejor predice la afectación de las cuentas y la pluralidad de la victimización.

Estos resultados son parcialmente consistentes con otros hallazgos de la literatura. Bernasco y Luykx (2003: 995), refiriendo resultados de hurto residencial de viviendas en Holanda, reportan la influencia del valor de la vivienda en la incidencia diferencial, y Meier y Miethe (1993: 483) refieren que el incremento del riesgo de victimización para personas de mayor nivel socioeconómico se observa en algunos estudios, aunque no en otros. Debe destacarse que estos resultados provienen de estudios sobre delincuencia contra la propiedad de tipo convencional, donde hay desplazamiento físico de delincuentes y donde otras variables situacionales, como exposición al delito y capacidad de custodia son diversas a las aplicadas al medio virtual. En otra evaluación sobre encuestas de victimización en Gran Bretaña, de 1982, estos últimos autores observaron que "no hay bases para sostener que el atractivo económico sea una condición necesaria para la victimización de tipo predatorio" (Miethe y Meier, 1990: 260).

En cuanto a la magnitud de la oportunidad, el nivel de vigilancia o supervisión de las cuentas, tal como lo predice la teoría, se encuentra negativamente asociado a la defraudación medida por el monto expuesto y por el agotamiento del fraude: a menor disponibilidad de perfil virtual, lo cual supone menos requisitos de ingreso y control sobre las cuentas, mayor probabilidad de incremento del monto expuesto, así como a mayor tiempo transcurrido entre la exposición del monto y la intervención preventiva del banco, lo que indica un menor nivel de supervisión, mayor la probabilidad del agotamiento del fraude. También el nivel de supervisión (o vigilancia) parece vincularse al fraude a través de la afectación preferente de cuentas en días cercanos a los no laborables, donde supuestamente el control de los empleados del banco es menor, así como en el caso en el cual no se activan las alertas parametrizadas, en el tramo de montos expuestos entre Bs. 1.000.000 y Bs. 5.000.000. Las transferencias ejecutadas a través de Internet, mayormente que las ejecutadas por vía telefónica, concluyen en el agotamiento del fraude, lo que indicaría que el nivel de supervisión y control, a través del contacto personalizado telefónico, puede ser un factor preventivo.

Las variables demográficas no predicen riesgo diferencial de fraude si se asocian a medidas de protección, pero sí se encuentran asociadas si se vinculan con el valor de la oportunidad. Ello quiere decir que la edad, el sexo, el nivel educativo y la ocupación no parecen tener valor independi-

ente en la explicación de dicha afectación, si se toman como condiciones personales de los titulares de las cuentas afectadas, sino a través del valor de la oportunidad que representan las cuentas de los titulares. Ello queda evidenciado en los análisis que hemos adelantado entre las variables demográficas y las variables consumación del fraude y tipo de victimización.

Esta investigación, a diferencia de la que reporta la literatura sobre las oportunidades delictivas, se ha desarrollado sobre victimización en el medio virtual, y en este sentido constituye un estudio novedoso. Las condiciones especiales de este medio probablemente determinan menor variabilidad de las condiciones de protección, asociadas a la magnitud de la oportunidad, dado que los procedimientos bancarios son más uniformes. Es posible que dicha menor variabilidad influya en que el valor del objeto del fraude, en nuestro caso estimado de acuerdo al monto depositado en las cuentas afectadas, resulte con un peso determinante y mayor del que generalmente reporta la literatura. Precisamente la variabilidad en las condiciones de protección podría estar asociada, en el caso del medio virtual, al comportamiento de las víctimas, y por ello pensamos que es importante adelantar investigación adicional sobre las características de las víctimas (para determinar conductas que incrementan el riesgo) y sobre infractores (para determinar los recursos del delincuente asociados al incremento de la oportunidad delictiva). Estos aspectos han sido destacados como importantes por la perspectiva de las oportunidades delictivas, y con la información estática de que se dispone en las bases de datos utilizadas para la presente investigación no es posible una aproximación a las conductas de las víctimas que pueden inhibir o favorecer la comisión del fraude, ni a las percepciones y disposiciones de los delincuentes para evaluar y vigilar a sus víctimas con la finalidad de escoger el blanco delictivo más atractivo. La identificación de víctimas y delincuentes relevantes para un estudio ulterior, sin embargo, puede representar desafíos y dificultades especiales, para cuya superación se requeriría arbitrar medios no invasivos y confidenciales para obtener información confiable preservando la identidad y la exposición de los informantes.

LISTA DE REFERENCIAS

BERNASCO, W. y LUYKX, F. (2003). "Effects of attractiveness opportunity and accessibility to burglars on residencial burglary rates of urban neighborhoods", **Criminology,** 41, 3, pp: 981- 1001.

BIRKBECK, C. (1984-1985). "El concepto de oportunidades para el delito: su definición y consecuencia". **Revista Cenipec** 9, pp. 43-81.

BIRKBECK, C. y LAFREE, G. (1988). "El análisis situacional del delito, con referencia a Venezuela y Estados Unidos", **Revista Cenipec** 11, pp. 55-83

BIRKBECK, C. y LAFREE, G. (1989). "Una revisión crítica de las teorías de las oportunidades para el delito". **Revista Cenipec** 12, pp. 11-34.

CENTRO INTERNACIONAL DE ESTUDIOS SUPERIORES DE COMUNICACIÓN PARA AMÉRICA LATINA (2001). Periscopio tecnológico: fin a la privacidad de los usuarios de Internet. Revista Latinoamericana de Comunicación Chasqui (76). Quito. Disponible en Internet: http://redalyc.uaemex. mx/redalyc/pdf/160/16007610.pdf

CLARKE, R.V. (1995). "Situational crime prevention", en M. Tonry y D.P. Farrington (editores) **Building a Safer Society : Strategic Approaches to Crime Prevention,** Chicago, University of Chicago Press, pp. 91-150.

FERNÁNDEZ, R. (2006). Reseña de la Jornada sobre Riesgos Penales de la Banca On-line [reseña en línea]. IDP. Revista de Internet, Derecho y Política (2). UOC. Disponible en Internet: http://www.uoc.edu/idp/2/dt/esp/fernandez.pdf

GABALDÓN, L.G., BENAVIDES, D., PARRA, Y. (2007). Victimización Delictiva y percepción de la policía, en L.G. Gabaldón y A. Antillano (editores) **La policía venezolana: desarrollo institucional y perspectivas de reforma al inicio del tercer milenio. Tomo I,** Caracas, Comisión Nacional para la Reforma Policial, pp. 307-341.

GABALDÓN, L. y MORENO, M.T. (2003). **El fraude electrónico en Venezuela: una aproximación a sus tendencias y modalidades**. Informe de la primera fase del proyecto de investigación Fraude electrónico, lealtad empresarial y cultura corporativa. Caracas. Centro de Investigaciones Jurídicas, Núcleo de Estudios sobre Delincuencia Económica. Universidad Católica Andrés Bello (mimeo).

GUERRERO, M. y SANTOS, J. (1993). **Fraude informático en la banca: aspectos criminológicos**. Bogotá: Jesma LTDA.

MANNING, P.K. (2004). "Lealtad de los empleados en la era de la información: observaciones sobre las relaciones entre lealtad y organización", en L. G. GABALDÓN. **Delincuencia económica y las tecnologías de la información.** Caracas: Universidad Católica Andrés Bello, pp. 15-40.

MEIER, R.F. y MIETHE, T.D. (1993). "Understanding Theories of Criminal Victimization" in Michael Tonry (editor) **Crime and Justice, A Review of Research.** Chicago, Chicago University Press, pp. 459-499.

MIETHE, T.D. y MEIER, R.F. (1990). "Opportunity, choice and criminal victimization: a test of a theoretical model", **Journal of Research in Crime and Delinquency,** 27, 3, pp. 243-266.

RINCÓN, E. (2004). Principios de Seguridad en Banca Electrónica, y la Ley 527 de 1999. Revista de Derecho Informático (70). Edita: Alfa-Redi. Disponible en Internet: http://www.alfa-redi.org/rdi-articulo.shtml?x=1098

RODRÍGUEZ, G. (2000). Formas de pago electrónicas: regulación y oportunidades. Trabajo presentado en el II Simposio de Modernización de las Gobernaciones Venezolanas, logros y tendencias. Revista de Derecho Informático (20). Edita: Alfa-Redi. Disponible en Internet: http://www.alfa-redi.org/rdi-articulo .shtml?x=435

SALAZAR, C. (2003). "La informática y su impacto social". **Monografías.com**. Disponible en Internet: http://www.monografias.com/trabajos14/informatica-social/informatica-social.shtml

SEGISTAN, M. (2003). El E-Banking: una realidad financiera. Revista de Derecho Informático (64). Edita: Alfa-Redi. Disponible en Internet: http://www.alfa-redi.org/rdi-articulo.shtml?x=1267

SMITH, A. (2006). Exploring security and comfort issues associated with online banking. **Int. J. Electronic Finance**, vol. 1 (1), pp. 18-48. Disponible en Internet: http://www.inderscience.com/storage/f491631112710852.pdf

UMBRÍA, L. (2006) *Movilización Electrónica Fraudulenta.* Caracas (Comunicación personal)

VENEZUELA (2001a). **Decreto con Fuerza de Ley General de Bancos y otras Instituciones Financieras** (2001). Gaceta Oficial de la República Bolivariana de Venezuela N° 5.555 del 13 de noviembre de 2001.

VENEZUELA (2001b). **Ley Especial contra Delitos Informáticos** (2001). Gaceta Oficial de la República Bolivariana de Venezuela N° 37.313 del 30 de octubre de 2001

WARR, M. (2001). "Crime and opportunity: a theoretical essay"; en MEIER, R., KENNEDY L. y SACCO, V. (2001). **The process and structure of crime: criminal events and crime analysis**. New Brunswick: Transaction Publishers.

WHITAKER, R. (1999). El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad. Barcelona, España: Paidós

WIKSTRÖM, P.O. (2006). "Personas, entornos y actos delictivos: mecanismos situacionales y explicación del delito", en GUZMAN DALBORA, J.L. y SERRANO MAÍLLO A. (editores). **Derecho penal y criminología como fundamento de la política criminal, Estudios en homenaje al Profesor Alfonso Serrano Gómez.** Madrid, Dykinson, pp: 509-551.

WÜEEST, C. (2005). Threats to online banking. Symantec Security Response. Dublin. Disponible en internet: http://www.symantec.com/avcenter/reference/threats.to.online.banking.pdf